(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年10 月9 日 (09.10.2003)

PCT

(10) 国際公開番号
WO 03/083646 A1

(51) 国際特許分類[7]: G06F 9/06, 13/00, H04M 11/00

(21) 国際出願番号: PCT/JP03/03974

(22) 国際出願日: 2003 年3 月28 日 (28.03.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-101756 2002 年4 月3 日 (03.04.2002) JP

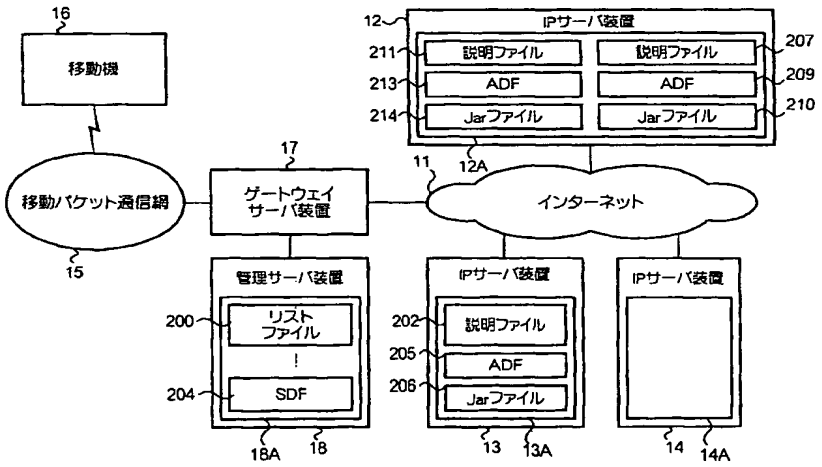
(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 渡邊 信之 (WATANABE,Nobuyuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 澤田 久徳 (SAWADA,Hisanori) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 西尾 英昭 (NISHIO,Hideaki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 中村 友則 (NAKAMURA,Tomonori) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 三浦 史光 (MIURA,Fumiaki) [JP/JP]; 〒100-6150 東京都 千

[続葉有]

(54) Title: DISTRIBUTION METHOD, DISTRIBUTION SYSTEM, AND TERMINAL DEVICE

(54) 発明の名称: 配信方法、配信システム及び端末装置



16...MOBILE DEVICE
15...MOBILE PACKET COMMUNICATION NETWORK
17...GATEWAY SERVER DEVICE
18...MANAGEMENT SERVER DEVICE
200...LIST FILE
12...IP SERVER DEVICE
211...EXPLANATION FILE
207...EXPLANATION FILE
214...Jar FILE
210...Jar FILE
11...INTERNET
13...IP SERVER DEVICE
202...EXPLANATION FILE
206...Jar FILE
14...IP SERVER DEVICE

(57) Abstract: A mobile device (16) capable of starting Java-AP software acquires an ADF (205) from an IP server device (13). By using the ADF (205), the mobile device (16) receives an SDF (security description file) (204) from a management server device (18) managed by a reliable organization (communication company managing a mobile packet communication network (15)). Next, by using the ADF (205), the mobile device (16) acquires a Jar file (206) from an IP server device (13). The mobile device (16) installs in itself Java-AP software containing these files. The Java-AP realized by starting the Java-AP software operates within a range of authority represented by the policy information included in the SDF (204).

[続葉有]

WO 03/083646 A1

代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 富岡 淳樹 (TOMIOKA,Atsuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

(74) 代理人: 川崎 研二 (KAWASAKI,Kenji); 〒103-0027 東京都 中央区 日本橋一丁目２番１０号 東洋ビルディング ７階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, JP, KR, NO, NZ, PH, PL, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: Ｊａｖａ−ＡＰソフトウェアを起動することができる移動機１６が、ＩＰサーバ装置１３からＡＤＦ２０５を取得し、このＡＤＦ２０５を用いて信頼できる機関（移動パケット通信網１５を管理する通信事業者）が管理する管理サーバ装置１８からＳＤＦ（セキュリティ記述ファイル）２０４を受信し、次いで、ＡＤＦ２０５を用いてＩＰサーバ装置１３からＪａｒファイル２０６を取得し、これらのファイルを内包するＪａｖａ−ＡＰソフトウェアを自身にインストールする。このＪａｖａ−ＡＰソフトウェアを起動することで実現されるＪａｖａ−ＡＰは、ＳＤＦ２０４に内包されているポリシー情報で表される権限の範囲内で動作する。

明細書

配信方法、配信システム及び端末装置

技術分野

本発明は、端末装置にアプリケーションソフトウェアを配信する技術に関する。

背景技術

Ｊａｖａ（登録商標）プログラミング言語に従って記述されたプログラムを実行してＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）を実行する機能と、この種のプログラムを含むＪａｖａ－ＡＰソフトウェアを、ネットワークを介してダウンロードする機能とを備えた移動機が普及している。

Ｊａｖａ－ＡＰソフトウェアとして、Ｊａｒ（Java Archive）ファイルとＡＤＦ（Application Descriptor File）とがある。ここで、Ｊａｒは、それが実行されることにより、あるＪａｖａ－ＡＰをユーザに提供するプログラムを内包している。また、ＡＤＦはＪａｒファイルに依存しており、例えば、Ｊａｒファイルの格納位置を示すＵＲＬ（以後、パッケージＵＲＬ）、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等を必須情報として内包している。

移動機は、次のような手順で、所望のＪａｖａ－ＡＰに関連したソフトウェアのダウンロードを行う。まず、移動機は、ＷＷＷ（World Wide Web）を構成するサーバ装置から所望のＪａｖａ－ＡＰに関連したＡＤＦを取得する。

ＡＤＦを取得した移動機はこのＡＤＦの内容を調べるとともに、その移動機に設けられたメモリの空き容量を調べ、所望のＪａｖａ－ＡＰに

関連したＪａｒファイルを当該移動機にインストール可能であるか否かを判断する。そして、インストール可能と判断すると、移動機は、ＡＤＦに含まれていたパッケージＵＲＬを用いて、ＷＷＷを構成するサーバ装置からＪａｒファイルを取得する。このＪａｒファイルには、Ｊａｖａ－ＡＰソフトウェアが格納されている。従って、このＪａｒファイルの取得をもってＪａｖａ－ＡＰソフトウェアのダウンロードは完了する。その後、移動機においては、ダウンロードされたＪａｖａ－ＡＰソフトウェアのインストールが行われ、当該Ｊａｖａ－ＡＰソフトウェアは起動要求さえあれば実行される状態となる。

ところで、移動機内で実行されるＪａｖａ－ＡＰの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、Ｊａｖａ－ＡＰは、移動機内の電話番号データなどの秘匿性の高い情報を参照することができないようになっている。このような厳しい制限を課すことにより、悪意をもって作成されたＪａｖａ－ＡＰ、あるいは不具合を有するＪａｖａ－ＡＰによって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

しかし、上述した厳しい制限を全てのＪａｖａ－ＡＰに対して一律に課すだけでは、ユーザやＩＰ（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、Ｊａｖａ－ＡＰに移動機に格納された個人情報を参照する権限を与えてもよいと感じるユーザがいると思われる。また、ＩＰにも、移動機に格納されている個人情報や移動機が有する多数の機能を使用する、より魅力的なＪａｖａ－ＡＰを提供したいという希望がある。

これらの希望を満たすべく、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関がＪａｖａ－ＡＰに権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該Ｊａｖａ－ＡＰの挙動を制限するという仕組みが考えられる。この仕組みで

は、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

Ｊａｖａ－ＡＰソフトウェアのダウンロード手順に上述の仕組みを適用する場合、信頼できる機関がＡＤＦあるいはＪａｒファイルに権限を示す情報を内包させるのが妥当である。ここで、ＪａｒファイルはＩＰにより随時更新されるので、ＩＰが保有するのが適当である。しかし、ＩＰがＪａｒファイルを保有するとすると、信頼できる機関はＪａｒファイルを保有し得ない。従って、信頼できる機関は、このようなＪａｒファイルよりは、むしろＡＤＦを保有し、このＡＤＦに権限を示す情報を内包させるのが妥当であるということができる。

しかし、ＡＤＦはＪａｒファイルに依存した内容となることから、ＩＰが手元のＪａｒファイルを更新すると、信頼できる機関が保有しているＡＤＦの更新も必要になってくる。ここで、信頼できる機関は、他社の関与を排するようにＡＤＦを管理することが必要であるから、信頼できる機関とＩＰが連携してＡＤＦを更新することとなり、その作業が繁雑なものになることが懸念される。また、Ｊａｒファイルを更新せずとも、ＡＤＦの更新が必要となることがある。例えば、ＩＰにおいて、あるＪａｒファイルへのアクセスが殺到し、このＪａｒファイルを他のサーバ装置へ移動する場合である。この場合、Ｊａｒファイルの格納位置が変更されるから、ＡＤＦに内包されているパッケージＵＲＬを変更する必要がある。しかしながら、ＡＤＦは信頼できる機関において他者の関与を排するように管理されるのであるから、ＡＤＦの更新作業は繁雑な作業となると予想される。

発明の開示

本発明は、上述した事情に鑑みて為されたものであり、権限に応じた挙動をアプリケーションに許可する端末装置に対し、依存関係にある複数のファイルを配信することによってそのアプリケーションを実現するためのソフトウェアを配信可能な仕組みを提供することを目的として

いる。

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、前記端末装置が、前記配信システムから送信されてくるアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信する過程と、前記端末装置が、前記配信システムから送信された前記アプリケーション記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程とを有する配信方法を提供する。

この方法によれば、配信システムが、アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、得たアプリケーション記述ファイルに内包されているセキュリティ記述ファイルの格納位置を配信システムに通知し、配信システムが、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装

置が、配信システムから送信されてくるアプリケーション記述ファイルに内包されている実体ファイルの格納位置を前記配信システムに通知し、配信システムが、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

また、本発明は、ネットワーク内の装置との通信を行うための通信部と、記憶部と、制御部とを具備し、前記制御部は、（ａ）アプリケーションを実現するためのソフトウェアを内包した実体ファイルの格納位置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルの格納位置を示す情報を含んだ第１の配信要求を前記通信部により前記ネットワーク内の配信システムに送信することにより、前記配信システムにおける情報提供サーバ装置に格納されたアプリケーション記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、（ｂ）前記配信システムから受信されたアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を示す情報を含んだ第２の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける管理サーバ装置に記憶されたセキュリティ記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、（ｃ）前記配信システムから受信されたアプリケーション記述ファイルに内包されている実体ファイルの格納位置を示す情報を含む第３の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける情報提供サーバに格納された実体ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、（ｄ）前記記憶部に記憶された実体ファイルに含まれるソフトウェアの実行が指示された場合に、前記記憶部に記憶された該実体ファイルに対応したセキュリティ記述ファイルに含まれる権限情報に従い、該ソフトウェアの実行により実現されるアプリケーションの挙動を制限する手

段とを有する端末装置を提供する。

この場合において、前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、前記端末装置の制御部は、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する手段を具備していてもよい。

また、前記端末装置の制御部は、前記通信部により、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを受信してもよい。

この場合において、前記端末装置の制御部は、暗号化通信により前記セキュリティ記述ファイルを受信してもよい。

また、前記端末装置の制御部は、前記通信部により、移動通信網および専用線を介して前記セキュリティ記述ファイルを受信してもよい。

この場合において、前記端末装置の制御部は、移動通信網を介した暗号化通信により前記セキュリティ記述ファイルを受信してもよい。

好ましい態様において、前記端末装置の制御部におけるアプリケーションの挙動を制限する手段は、前記セキュリティ記述ファイルに内包された権限情報に基づき、資源の利用を制限してもよい。

この場合において、前記資源は前記端末装置内部のハードウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なハードウェア資源であってもよいし、前記端末装置内部のソフトウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源であってもよいし、前記端末装置が使用可能なネットワーク資源であってもよい。

好ましい態様において、前記端末装置の制御部におけるアプリケーションの挙動を制限する手段は、前記権限情報に基づき資源の利用の種類を判断してもよい。

好ましい態様において、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、前記セ

キュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、前記制御部は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する端末装置を提供する。

また、好ましい態様において、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、前記制御部は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する端末装置を提供する。

また、前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記端末装置の制御部は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するようにしてもよい。

好ましい態様において、前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、前記端末装置の制御部は、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから当該セキュリティ記述ファイルが時系列的に繰り返し受信し、繰り返し受信される前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する手段を具備していてもよい。

この場合、前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてきた場合にのみ、前記アプリケーションの有効期限を更新するようにしてもよい。

好ましい態様において、前記端末装置は移動機であってもよい。

また、本発明はアプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した１または複数のサーバ装置とを有し、前記１または複数のサーバ装置のうち前記セキュリティ記述ファイルを格納するサーバ装置は、セキュリティ記述ファイルを管理する権限の与えられた管理サーバ装置であり、各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送する手段を有し、前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する配信システムを提供する。

図面の簡単な説明

図１は本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

図２は同システムに特有のＡＤＦのデータ構成を示す概念図である。

図３は同システムにおいて管理サーバ装置に格納されているＳＤＦのデータ構成を示す概念図である。

図４は同ＳＤＦに内包されるポリシー情報の内容を示す概念図である。

図５は同システムを構成する移動機の構成を示すブロック図である。

図６は同移動機の機能構成を示す概念図である。

図７は同移動機がＪａｖａ－ＡＰソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

図８は同移動機がＪａｖａ－ＡＰソフトウェアの有効期限を更新す

る処理の流れを示すフローチャートである。

図９は同配信システムの動作を説明するためのブロック図である。

図１０は同配信システムにて配信されるリストページを示す図である。

図１１は同配信システムを構成するＩＰサーバ装置が格納している説明ファイルの内容を示す図である。

図１２は同配信システムにて配信される説明ページを示す図である。

図１３は同ＩＰサーバ装置が格納している説明ファイルの内容を示す図である。

図１４は同配信システムにて配信される説明ページを示す図である。

図１５は同配信システムを構成するＩＰサーバ装置１３が格納している説明ファイルの内容を示す図である。

図１６は同配信システムにて配信される説明ページを示す図である。

図１７は同配信システムの動作を説明するためのシーケンス図である。

図１８は同配信システムの動作を説明するためのシーケンス図である。

図１９は同配信システムの動作を説明するためのシーケンス図である。

図２０は同配信システムの動作を説明するためのシーケンス図である。

図２１は移動機にて表示される画面を示す図である。

図２２は同配信システムの他の動作を説明するためのブロック図である。

図２３は同配信システムの他の動作を説明するためのシーケンス図である。

図２４は、ＳＤＦの有効性を問い合わせるための処理を行う移動機の制御部内の構成を示す図である。

図２５は、ＳＤＦの有効性の問い合わせの動作を示すタイムチャート

である。

発明を実施するための最良の形態

以下、図面を参照して、本発明の実施の一形態である配信システムについて説明する。なお、図面において、共通する部分には同一の符号が付されている。

（１）構成

図１に示されるように、この配信システムにおいて、ＩＰサーバ装置１２～１４は、インターネット１１に接続されている。ＩＰサーバ装置１２は第１のＩＰ（Internet Provider）によって管理されており、ＩＰサーバ装置１３および１４は第１のＩＰと異なる第２のＩＰにより管理されている。そして、ＩＰサーバ装置１２～１４はＷＷＷを構成しており、それぞれ一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。移動パケット通信網１５は、通信事業者が移動パケット通信サービスを提供するために用いる網である。移動機１６は、この移動パケット通信網１５との間で無線パケット通信を行うことが可能である。ゲートウェイサーバ装置１７は、移動パケット通信網１５と同じ通信事業者により管理されている。このゲートウェイサーバ装置１７は、移動パケット通信網１５とインターネット１１とを接続する装置であり、一般的なゲートウェイサーバ装置の構成と同様の構成を有する。管理サーバ装置１８は、専用線によりゲートウェイサーバ装置１７に接続されている。この管理サーバ装置１８もまたＷＷＷを構成し、一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。ゲートウェイサーバ装置１７は、移動パケット通信網１５とインターネット１１との間のパケット中継、管理サーバ装置１８と移動パケット通信網１５との間のパケット中継および管理サーバ装置１８とインターネット１１との間のパケット中継を行う。移動機１６は、この中継機能を利用することにより、移動パケット通信網１５およびインターネット１１を介してＩＰサーバ装置１２～１４とパケット通信を行うことが可能で

ある。なお、実際の配信システムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機１６のみが図示されている。これと同様の理由により、３つのＩＰサーバ装置１２～１４のみが図示されている。

この配信システムにおいて、移動機１６は、インターネット１１上の所望のサイトからＪａｖａ－ＡＰソフトウェアを受け取ることができる。この移動機１６が受け取ることができるソフトウェアは、トラステッドＪａｖａ－ＡＰに関するものと、非トラステッドＪａｖａ－ＡＰに関するものに大別される。ここで、トラステッドＪａｖａ－ＡＰソフトウェアは、移動パケット通信網１５を管理する通信事業者が、ＩＰサーバ装置１２～１４を管理するＩＰとの契約に基づいて信頼性を保証したＪａｖａ－ＡＰソフトウェアである。また、非トラステッドＪａｖａ－ＡＰソフトウェアは、トラステッドＪａｖａ－ＡＰソフトウェア以外のＪａｖａ－ＡＰソフトウェアである。

管理サーバ装置１８は、この配信システム内を流通する各トラステッドＪａｖａ－ＡＰソフトウェアについてＳＤＦ（セキュリティ記述ファイル）を各々記憶している。このＳＤＦは、移動パケット通信網１５を管理する通信事業者によって作成されるファイルであり、移動機のトラステッドＡＰＩ（APplication Interface）を使用するＪａｖａ－ＡＰソフトウェアを移動機にダウンロードする際に必須のファイルである。なお、トラステッドＡＰＩについては後述する。図３に示されるように、ＳＤＦは、トラステッドＪａｖａ－ＡＰソフトウェアを識別するためのＡＰＩＤ、ポリシー情報、および有効期限を有する。これらの情報は通信事業者の秘密鍵を用いて暗号化されている。ここで、ポリシー情報は、トラステッドＪａｖａ－ＡＰの移動機１６内での挙動に対する制限を示す情報である。なお、このポリシー情報およびこれに基づいて行われるＪａｖａ－ＡＰの挙動の制限の詳細については後述する。

本実施形態では、移動機１６から所望のトラステッドＪａｖａ－ＡＰソフトウェアの配信要求が送信された場合に、ＩＰサーバ装置１２～１

４の１つから移動機１６にそのトラステッドＪａｖａ－ＡＰソフトウェアにおけるＡＤＦが配信される。ここで、トラステッドＪａｖａ－ＡＰソフトウェアのＡＤＦには、Ｊａｒファイルの所在を示すＵＲＬの他、このトラステッドＪａｖａ－ＡＰソフトウェアに対応したＳＤＦの所在を示すＵＲＬと、そのＳＤＦの暗号化に用いられた秘密鍵と対をなす公開鍵が含まれている。このＡＤＦを受信した移動機１６は、ＡＤＦ内のＵＲＬを用いてＳＤＦを取得し、ＡＤＦ内の公開鍵を用いてＳＤＦを復号化する。そして、最後に移動機１６は、ＡＤＦに含まれているＪａｒファイルのＵＲＬを用いて、Ｊａｒファイルを取得する。その後、移動機１６において、トラステッドＪａｖａ－ＡＰソフトウェアが実行されるときには、ＳＤＦに基づいて、トラステッドＪａｖａ－ＡＰの挙動の制限が行われる。これが本実施形態の特徴の１つである。図１に示すとおり、ＳＤＦの送信は移動パケット通信網１５を通して行われ、管理サーバ装置１８とゲートウェイサーバ装置１７は専用線によって接続されている。

以下、この特徴との関連において、配信システムの各要素の構成を説明する。

ＩＰサーバ装置１２、１３及び１４は不揮発性メモリ１２Ａ，１３Ａ及び１４Ａをそれぞれ有する。

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａは、ハードディスク等の不揮発性メモリであり、Ｊａｒファイルおよびａｄｆからなるｊａｖａ－ＡＰソフトウェアと、Ｊａｖａ－ＡＰソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶している。

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａに記憶されている個々のＪａｖａ－ＡＰソフトウェアは、トラステッドＪａｖａ－ＡＰソフトウェアであるかも知れないし、非トラステッドＪａｖａ－ＡＰソフトウェアであるかも知れない。トラステッドＪａｖａ－ＡＰであるか非トラステッドＪａｖａ－ＡＰであるかに拘わらず、全てのＪａｖａ－ＡＰソフトウェアのＡＤＦには、ＷＷＷにおけるＪａｒファイルの記憶位置を示

すパッケージＵＲＬや、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等が記述されている。これらはＪａｖａ－ＡＰソフトウェアのＡＤＦに記述されるべき項目として一般的に知られているものである。そして、トラステッドＪａｖａ－ＡＰソフトウェアのＡＤＦは、これらの一般的に知られた情報の他に、図２に示されるように、そのトラステッドＪａｖａ－ＡＰソフトウェアのＡＰＩＤと、Ｊａｒファイルのハッシュ値と、ＳＤＦがＷＷＷにおいて記憶されている位置を示すＵＲＬ（以下、ＳＤＦ－ＵＲＬと呼ぶ）と、そのＳＤＦの暗号化に使用された秘密鍵と対をなす公開鍵とを内包している。ここで、公開鍵は、図示せぬＣＡ（認証局）によって正当性が証明された通信事業者に対し、証明書として発行されるものである。

また、説明ファイルは、ＨＴＭＬに従って記述されたテキストファイルである。移動機は、あるＪａｖａ－ＡＰソフトウェアをダウンロードする場合に、それに先だって、このＪａｖａ－ＡＰソフトウェアに対応した説明ファイルをダウンロードする必要がある。説明ファイルには、Ｊａｖａ－ＡＰソフトウェアのダウンロードの指示をユーザから受け取るＵＩ（ユーザインターフェイス）を構成するための情報が含まれている。移動機１６は、この情報に従い、ＵＩ画面を表示する。ユーザは、このＵＩ画面中の所望のＪａｖａ－ＡＰを表すオブジェクトを指定する操作を移動機１６に対して行うことができる。説明ファイルには、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるＪａｖａ－ＡＰソフトウェアに対応するＡＤＦのＷＷＷにおける所在を示すＵＲＬに対応付けるように記述されている。

ＩＰサーバ装置１２～１４の各々は、以上説明した各ファイルをＩＰの指示に従って作成および更新する機能を備えている。

管理サーバ装置１８は、ハードディスク等の不揮発性メモリ１８Ａを有する。管理サーバ装置１８は、ＴＣＰコネクションを通信相手との間に確立する。管理サーバ装置１８は、このＴＣＰコネクションを介して、ＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを通信相手から受

信すると、当該ＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを不揮発性メモリ１８Ａから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送して当該コネクションを切断する。

また、上記不揮発性メモリ１８Ａには、ダウンロード可能なＪａｖａ－ＡＰソフトウェアを移動機１６のユーザに紹介するためのリストファイル２００と、このリストファイル２００に挙げられた各Ｊａｖａ－ＡＰソフトウェアに各々対応したＳＤＦとが記憶される。

これらのうちＳＤＦは、既に図３を参照して説明した通りである。

リストファイル２００は、ＨＴＭＬに従って記述されたテキストファイルである。既に説明したように、移動機は、あるＪａｖａ－ＡＰソフトウェアをダウンロードする場合に、それに関連した説明ファイルを取得する必要がある。既に説明したように、移動機１６は、この説明ファイルを格納しているＩＰサーバ装置にアクセスするという方法により、この説明ファイルを取得することができる。しかし、このような直接的な方法以外に、本実施形態において移動機１６は、次のような手順により所望のＪａｖａ－ＡＰソフトウェアの説明ファイルを取得することもできる。まず、移動機１６は、管理サーバ装置１８にアクセスして、このリストファイル２００を取得し、これに従い、ＵＩ画面を表示する。ユーザは、このＵＩ画面中の所望のＪａｖａ－ＡＰを表すオブジェクトを指定する操作を移動機１６に対して行うことができる。リストファイル２００は、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるＪａｖａ－ＡＰソフトウェアの説明ファイルのＷＷＷにおける所在を示すＵＲＬに対応付ける。移動機１６は、このようにリストファイル２００を介して得られるＵＲＬを用いて、ＩＰサーバ装置から説明ファイルを取得するのである。

移動機１６は、図５に示されるように、ＯＳ（オペレーティングシステム）ソフトウェア、Ｊａｖａ－ＡＰを実行する環境を構築するためのＪａｖａ－ＡＰ環境ソフトウェアおよび各種ネイティブＡＰソフトウェア等を記憶したＲＯＭ１６Ａと、ＲＯＭ１６Ａに接続されＲＯＭ１６

Aからプログラムを読み出して実行するＣＰＵ１６Ｂと、ＣＰＵ１６Ｂに接続された表示部１６Ｃと、不揮発性メモリ１６Ｄと、ＲＡＭ１６Ｅと、通信部１６Ｆと、操作部１６Ｇとを有する。

表示部１６Ｃは、例えば液晶表示パネルを有し、ＣＰＵ１６Ｂから供給されるデータを画像として表示する。不揮発性メモリ１６Ｄは例えばＳＲＡＭやＥＥＰＲＯＭであり、ＣＰＵ１６Ｂによりデータを読み書きされる。不揮発性メモリ１６Ｄは、WWWを構成するサーバ装置（以後、Ｗｅｂサーバ装置）からダウンロードしたＪａｖａ－ＡＰソフトウェアを記憶するために使用される。既に述べたように、本実施形態において、「Ｊａｖａ－ＡＰソフトウェア」という語は、「トラステッドＪａｖａ－ＡＰソフトウェア」および「非トラステッドＪａｖａ－ＡＰソフトウェア」の両方を指すのに用いられている。しかし、ある文脈において「Ｊａｖａ－ＡＰソフトウェア」という語が「トラステッドＪａｖａ－ＡＰソフトウェア」を指している場合もある。そのような文脈において、この語は、ＡＤＦ、ＳＤＦおよびＪａｒを含む概念と解釈されるべきである。また、ある文脈において、「Ｊａｖａ－ＡＰソフトウェア」という語が「非トラステッドＪａｖａ－ＡＰソフトウェア」を指している場合もある。そのような文脈において、この語はＡＤＦおよびＪａｒを含む概念と解釈されるべきである。

通信部１６Ｆは、移動パケット通信網１５と無線パケット通信を行うものであり、ＣＰＵ１６Ｂと移動パケット通信網１５との間でパケットを中継する。また、通信部１６Ｆは、アンテナや無線送受信部の他に、通話のためのＣＯＤＥＣやマイク、スピーカ等を備えている。従って、移動機１６は、この通信部１６Ｆにより、図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部１６Ｇは操作子を備え、操作子の操作に応じた信号をＣＰＵ１６Ｂへ供給する。計時部１６Ｈは、現在の年月日および時刻（以下、単に現在日時という）を計時する。なお、計時部１６Ｈがより正確な現在日時を計時するために、例えば移動パケット通信網１５の図示せぬ基地局から制御チャネルを介して定期

的に通知される現在日時に同期させるような処理を行ってもよい。

ＣＰＵ１６Ｂは、ＲＯＭ１６Ａに記憶された各種プログラムに従って移動機１６全体の制御を行う装置である。図示せぬ電源が投入されると、このＣＰＵ１６ＢはＲＡＭ１６Ｅをワークエリアとし、ＲＯＭ１６Ａから図６のＯＳを読み出して実行する。ＣＰＵ１６Ｂは、このＯＳに従ってＵＩ等を機能を提供する。ＯＳは操作部１６Ｇから供給される信号とＵＩの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

ユーザの指示がネイティブＡＰソフトウェアである通信ソフトウェアの起動を要求するものであれば、ＯＳは通信ソフトウェアを起動して移動機１６内にて通信ＡＰを実行する。この通信ＡＰを用いることで、ユーザは通話相手と通話をすることができる。

ユーザの指示がネイティブＡＰソフトウェアである電話帳ＡＰの起動を要求するものであれば、ＯＳは電話帳ソフトウェアを起動して移動機１６内にて電話帳ＡＰを実行する。この電話帳ＡＰを用いることで、ユーザは、不揮発性メモリ１６Ｄに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

ユーザの指示がネイティブＡＰソフトウェアであるＷｅｂブラウザソフトウェアの起動を要求するものであれば、ＯＳはＷｅｂブラウザソフトウェアを起動して移動機１６内にてＷｅｂブラウザを実行する。このＷｅｂブラウザはＵＩを提供する。そして、Ｗｅｂブラウザは、ユーザから操作部１６Ｇの操作により指示があると、ＵＩの状態と操作部１６Ｇから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイルをＷＷＷから取得する旨の場合には、通信部１６Ｆを制御して当該ファイルを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、このコネクションを介して、指定された位置を示すＵＲＬをＧＥＴメソッドに用いたＨＴＴＰの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、

ＷｅｂブラウザはＷｅｂページを内包するＵＩを生成し、ユーザに提供する。また、ユーザの指示がＪａｖａ－ＡＰソフトウェアのダウンロードを要求するものである場合には、Ｗｅｂブラウザは、この指示を次に述べるＪＡＭ（Java Application Manager）に通知する。具体的には、Ｗｅｂページにおいて、クリック操作またはプレス操作により、オブジェクトタグが指定されているアンカータグで表されるアンカーが指定されると、Ｗｅｂブラウザは当該オブジェクトタグのｄａｔａ属性に指定されているＵＲＬを抽出し、当該ＵＲＬからのＪａｖａ－ＡＰソフトウェアのダウンロードが要求されたことをＪＡＭに通知する。

ユーザの指示がネイティブＡＰソフトウェアであるＪＡＭソフトウェアの起動を要求するものであれば、ＯＳはＪＡＭソフトウェアを起動して移動機１６内にてＪＡＭを実行する。ＪＡＭは、移動機１６にインストールされているＪａｖａ－ＡＰソフトウェアの一覧をユーザに提示し、ユーザにより指定されたＪａｖａ－ＡＰソフトウェアを起動する。具体的には、ＪＡＭに対するユーザの指示がＪａｖａ－ＡＰソフトウェアの起動を要求するものであれば、Ｊａｖａ－ＡＰ環境ソフトウェアが起動されて移動機１６内にＪａｖａ－ＡＰ環境が実行される。そして、指定されたＪａｖａ－ＡＰソフトウェアが起動されてＪａｖａ－ＡＰ環境内にＪａｖａ－ＡＰが実行される。Ｊａｖａ－ＡＰ環境は、携帯端末に適した軽量のＪａｖａ仮想マシンであるＫＶＭと、Ｊａｖａ－ＡＰに対して提供されるＡＰＩとを有する。Ｊａｖａ－ＡＰに対して提供されるＡＰＩは、通信事業者がＩＰとの契約に基づいて信頼性を保証したＪａｖａ－ＡＰ（以後、トラステッドＡＰ）のみに使用が許可されるトラステッドＡＰＩと、あらゆるＪａｖａ－ＡＰに使用が許可される非トラステッドＡＰＩとに分けられる。

（２）動作

以下、本実施形態の動作を説明する。

（２－１）移動機１６によるＪａｖａ－ＡＰソフトウェアのダウンロー

ド

ＪＡＭは、Ｊａｖａ－ＡＰのダウンロードを要求する指示がＷｅｂブラウザから通知されると、Ｊａｖａ－ＡＰソフトウェアを移動機１６にダウンロードしインストールする処理を行う。この処理の流れを図７に示す。なお、図７では、移動機１６が説明ファイルを取得するまでの過程は省略されている。説明ファイルの取得までの過程は、幾つかの態様があるので、後に具体的な動作例を挙げて説明する。図７に示されるように、ＪＡＭは、まず、Ｊａｖａ－ＡＰソフトウェアのダウンロードを要求する指示があったか否かを判定する（ステップＳ１１）。そして、Ｊａｖａ－ＡＰソフトウェアのダウンロードを要求する指示がＷｅｂブラウザから通知されると、そのＪａｖａ－ＡＰソフトウェアに対応するＡＤＦをＩＰサーバ装置１２～１４のいずれかから取得する（ステップＳ１２）。具体的には、ＪＡＭは、ＩＰサーバ装置１２～１４のうちＡＤＦを格納しているものとの間にＴＣＰコネクションを確立し、ＡＤＦの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＡＤＦを取得した後、このＴＣＰコネクションを切断する。そして、ＪＡＭは、応答メッセージに内包されているＡＤＦを不揮発性メモリ１６Ｄに書き込む。

次いで、ＪＡＭは、ダウンロードしようとしているＪａｖａ－ＡＰソフトウェアを移動機１６にインストール可能か否かをＡＤＦの内容に基づいて判定する（ステップＳ１３）。ここでは、ＡＤＦに記述されていたＪａｒファイルのサイズと、不揮発性メモリ１６Ｄ内のＪａｒファイルを記憶可能な空き容量とを比較する等の、従来と同様の基準に従って判定すればよい。

ここで、インストール可能と判定された場合には（ステップＳ１３；Ｙｅｓ）、ＪＡＭは、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアであるか否かを判定する（ステップＳ１４）。具体的には、ＪＡＭは、ステップＳ１２において取得したＡＤＦ内にＳＤＦ－ＵＲＬが記述されているか否かを

確認し、記述されていれば、このＪａｖａ－ａｐソフトウェアに対応するＳＤＦが存在する、即ち、トラステッドＪａｖａ－ＡＰソフトウェアであると判定するし、その記述がなければ非トラステッドＪａｖａ－ＡＰソフトウェアであると判定する。

そして、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアが非トラステッドＪａｖａ－ＡＰソフトウェアであると判定された場合には（ステップＳ１４；Ｎｏ）、従来と同様のダウンロードおよびインストール処理が行われる（ステップＳ１５）。

一方、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアと判定された場合には（ステップＳ１４；Ｙｅｓ）、ＪＡＭは、このソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得する（ステップＳ１６）。すなわち、ＪＡＭは、管理サーバ装置１８との間にＴＣＰコネクションを確立し、このコネクションを介して、ＡＤＦ内に記述されているＳＤＦ－ＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＳＤＦを取得した後、上記コネクションを切断する。

前述したように、トラステッドＪａｖａ－ＡＰソフトウェアに対応するＳＤＦは、ＡＰＩＤとポリシー情報と有効期限とを内包し、さらに通信事業者の秘密鍵により署名（暗号化）されている。そこで、ＪＡＭは、応答メッセージに内包されているＳＤＦの署名を、既に取得しているＡＤＦから抽出された公開鍵を用いて検証し（復号し）、このＳＤＦの正当性を判断する（ステップＳ１７）。正当性が確認された場合（ステップＳ１７；Ｙｅｓ）、ＪＡＭは、ＳＤＦを不揮発性メモリ１６Ｄに書き込む。

次いで、ＪＡＭは、ＳＤＦに内包されているＡＰＩＤと、既に取得しているＡＤＦに内包されていたＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ１８）。

両者が一致すると判定された場合には（ステップＳ１８；Ｙｅｓ）、

ＪＡＭは、Ｊａｒファイルを取得する（ステップＳ１９）。具体的には、ＪＡＭは、ＡＤＦに内包されているパッケージＵＲＬで特定されるＪａｒファイルを記憶したＩＰサーバ装置１２～１４のいずれかとの間にＴＣＰコネクションを確立し、このＪａｒファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＪａｒファイルを取得し、このＴＣＰコネクションを切断する。

次に、ＪＡＭは、取得したＪａｒファイルに対するハッシュ値を算出する（ステップＳ２０）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機１６で使用されるハッシュ関数とＡＤＦに含まれるハッシュ値の算出時に使用されるハッシュ関数とは一致していなければならない。実際には、移動機１６で使用されるハッシュ関数を用いて、トラステッドＪａｖａ－ＡＰソフトウェアを提供するＩＰがハッシュ値を算出してＡＤＦを生成することになる。

ＪＡＭは、算出したハッシュ値とＡＤＦから抽出したハッシュ値とを比較し、両者が一致した場合には（ステップＳ２１；Ｙｅｓ）、取得したＪａｒファイルを不揮発性メモリ１６Ｄに書き込み、トラステッドＪａｖａ－ＡＰソフトウェアのインストールに係る各種処理を行い（ステップＳ２２）、インストールに成功した旨をユーザに通知する（ステップＳ２３）。

以降、ＪＡＭは、トラステッドＪａｖａ－ＡＰソフトウェアを実行するに際し、トラステッドＪａｖａ－ＡＰの挙動を監視し、トラステッドＡＰＩの使用を制限するが、この制限は不揮発性メモリ１６Ｄに記憶されるＳＤＦ内のポリシー情報に従って行われることとなる。

なお、Ｊａｖａ－ＡＰソフトウェアをインストール不可能と判断された場合（ステップＳ１３；Ｎｏ）、ＳＤＦが正当でないと判断した場合（ステップＳ１７；Ｎｏ）、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合（ステップＳ１８；Ｎｏ）、算出したハッシュ値とＡＤＦが有するハッシュ値とが不一致の場合（ステップＳ２１；Ｎ

ｏ）には、ＪＡＭは、インストールに失敗した旨をユーザに通知するとともに、移動機１６の状態をステップＳ１１以前の状態に戻す。

（２－２）移動機１６によるＳＤＦの更新

トラステッドＪａｖａ－ＡＰソフトウェアは、対応するＳＤＦに内包されていた有効期限が経過するまでは移動機１６によって実行可能である。この有効期限を更新する場合には、移動機１６は、管理サーバ１８から新たにＳＤＦを取得する必要がある。そこで、以下では、ＪＡＭが、ＳＤＦ内の有効期限が到来する度にその有効期限を更新する場合の処理について、図８に示すフローを参照しながら説明する。

図８に示されるように、ＪＡＭは、移動機１６内の計時部１６Ｈによって計時される現在日時と、今までに取得した全てのＳＤＦからそれぞれ抽出して不揮発性メモリ１６Ｄに記憶した複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している（ステップＳ３１）。

いずれか１つでも有効期限が到来すると（ステップＳ３１；Ｙｅｓ）、ＪＡＭは、有効期限が到来したＪａｖａ－ＡＰソフトウェアの名称とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部１６Ｃに表示してユーザの操作があるまで待機する。

ユーザが有効期限を更新することを指示する操作を行うと、ＪＡＭはこの指示内容を解釈し（ステップＳ３２；Ｙｅｓ）、この有効期限を更新すべきＪａｖａ－ＡＰソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得する（ステップＳ３３）。具体的には、ＪＡＭは、不揮発性メモリ１６Ｄの記憶内容を参照し、有効期限を更新すべきＪａｖａ－ＡＰソフトウェアのＡＰＩＤを内包したＡＤＦに内包されているＳＤＦ－ＵＲＬを抽出し、このＳＤＦ－ＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し

てＳＤＦを取得した後、上記コネクションを切断する。

次いで、ＪＡＭは、上記ＳＤＦ－ＵＲＬを用いてＳＤＦを取得できたか否かを判断する（ステップＳ３４）。ここで、ＳＤＦを取得できない場合とは、何らかの事情でＪａｖａ－ＡＰソフトウェアの使用を中断或いは中止させたいという理由から、通信事業者が、管理サーバ装置１８において上記のＳＤＦ－ＵＲＬによって示される位置にＳＤＦを記憶させていないことを意味している。その事情とは、例えば、ＩＰの都合によってＪａｖａ－ＡＰソフトウェアの使用を中止或いは中断させたい場合（例えば、ユーザが一定期間だけ試用できるソフトウェアを配信するような場合）や、ＩＰと通信事業者との間で締結されていた契約が失効した場合等である。

さて、ＪＡＭは、ＳＤＦの取得に成功すると（ステップＳ３４；Ｙｅｓ）、ＳＤＦの署名を、既に取得しているＡＤＦに内包されている公開鍵を用いて検証し（復号し）、このＳＤＦの正当性を判断する（ステップＳ３５）。

正当性が確認されると（ステップＳ３５；Ｙｅｓ）、ＪＡＭは、ＳＤＦに内包されているＡＰＩＤと、既に取得済みのＡＤＦに内包されているＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ３６）。両者が一致すると判定された場合には（ステップＳ３６；Ｙｅｓ）、ＪＡＭは、取得したＳＤＦを不揮発性メモリ１６Ｄに既に書き込まれている以前のＳＤＦに上書きし、これにより有効期限を更新する。

なお、ユーザの操作により有効期限を更新しないと判断された場合（ステップＳ３２；Ｎｏ）、ＳＤＦを取得できなかった場合（ステップＳ３４；Ｎｏ）、ＳＤＦが正当でないと判断した場合（ステップＳ３５；Ｎｏ）、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合（ステップＳ３６；Ｎｏ）、ＪＡＭは、有効期限を更新しない旨をユーザに通知するとともに、移動機１６の状態をステップＳ３１以前の状態に戻す。

（３）具体的動作

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、ＴＣＰコネクションの確立および切断動作についてはＨＴＴＰにおける一般的な動作となることから、それらの説明を省略する。また、前述のＯＳ、Ｗｅｂブラウザ、ＪＡＭ、Ｊａｖａ－ＡＰ、ネイティブＡＰ等が行う動作は移動機１６の動作となることから、以降の説明では、動作の主体を移動機１６とする。

また、図９に示されるように、管理サーバ装置１８の不揮発性メモリ１８Ａには、リストファイル２００とＳＤＦ２０４が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰと管理サーバ装置１８を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されている。

これらのうち、リストファイル２００は、移動機１６において解釈・実行されると図１０に示されるリストページ２０１を提供するように記述されている。また、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ａが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０２のＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ｂが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０７のＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

また、ＳＤＦ２０４は、ＡＰＩＤとして“0001”、ポリシー情報として図４に示される内容の情報、有効期限として“２００２年１０月１日午前１０時”を内包しており、これらは通信事業者の秘密鍵を用いて署名されている。

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「詰め将棋」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例では、第１

の非トラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２１１の内容は図１１に示される通りであり、移動機１６において解釈・実行されると図１２に示される説明ページ２１２を提供するように記述されている。また、ＡＤＦ２１３はパッケージＵＲＬとしてＪａｒファイル２１４のＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）を内包している。

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「星占い」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例では、第２の非トラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２０７の内容は図１３に示される通りであり、移動機１６において解釈・実行されると図１４に示される説明ページ２０８を提供するように記述されている。また、ＡＤＦ２０９はパッケージＵＲＬとしてＪａｒファイル２１０のＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

なお、上述した第１の非トラステッドＪａｖａ－ＡＰソフトウェアと第２の非トラステッドＪａｖａ－ＡＰソフトウェアの違いは、後者に関連する情報がリストファイル２００に登録されているのに対し、前者に関連する情報が登録されていない点にある。

また、ＩＰサーバ装置１３の不揮発性メモリ１３Ａには、「電話帳ビューア」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例ではトラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明ファイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰによって作成されている。これらのうち、説明ファイル２０２の内容は図１５に示される通りであり、移動機１６において解

釈・実行されると図１６に示される説明ページ２０３を提供するように記述されている。ＡＤＦ２０５は、ＡＰＩＤとして“0001”、ハッシュ値としてＪａｒファイル２０６のハッシュ値、パッケージＵＲＬとしてＪａｒファイル２０６のＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）、ＳＤＦ－ＵＲＬとしてＳＤＦ２０４のＵＲＬ（“http://www.aaa.co.jp/viewer.sdf”）、及び通信事業者の公開鍵を内包している。また、移動機１６は上述の各Ｊａｖａ－ＡＰソフトウェアをインストール可能な状態にあるものとする。

（３－１）インストール動作

まず、Ｊａｖａ－ＡＰソフトウェアを移動機１６にインストールする場合の動作例について、上述したＪａｖａ－ＡＰソフトウェア毎に説明する。

（３－１－１）第１の非トラステッドＪａｖａ－ＡＰソフトウェア

第１の非トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２１１の取得を試みることから始まる。これにより、移動機１６では、説明ファイル２１１のＵＲＬ（“http://www.ccc.co.jp/mno.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ１２が生成される。この要求メッセージｔｍ１２は、図１７に示されるように、移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１２の内容に対応して説明ファイル２１１を内包した応答メッセージｔｍ１３が生成される。この応答メッセージｔｍ１３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２１１の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１２に示すような説明ページ２１２が表示される。

この説明ページ２１２を視たユーザが、説明ページ２１２内のアンカー２１２Ａが押下されるよう移動機１６を操作すると、移動機１６では、

図１１の説明ファイル２１１に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/shogi.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２１３の送信を要求する内容の要求メッセージｔｍ１６が生成される。この要求メッセージｔｍ１６は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１６の内容に対応してＡＤＦ２１３を内包した応答メッセージｔｍ１７が生成される。この応答メッセージｔｍ１７はＩＰサーバ装置１２から送信され移動機１６により受信される。

移動機１６では、ＡＤＦ２１３の内容に基づいて第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

次に、移動機１６では、ＡＤＦ２１３が不揮発性メモリ１６Ｄに書き込まれる。また、移動機１６では、ＡＤＦ２１３からパッケージＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１４の送信を要求する内容の要求メッセージｔｍ１８が生成される。この要求メッセージｔｍ１８は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１８の内容に対応してＪａｒファイル２１４を内包した応答メッセージｔｍ１９が生成される。この応答メッセージｔｍ１９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１４が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、

第１の非トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態はＡＤＦ２１３の取得を開始する前の状態に戻る。

（３－１－２）第２の非トラステッドＪａｖａ－ＡＰソフトウェア

第２の非トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０７またはリストファイル２００の取得を試みることから始まる。説明ファイル２０７の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル２００の取得を試みることから始まる動作のみについて説明する。

図１８に示されるように、移動機１６では、リストファイル２００のＵＲＬ（“http://www.aaa.co.jp/def.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２０が生成される。この要求メッセージｔｍ２０は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ２０の内容に対応してリストファイル２００を内包した応答メッセージｔｍ２１が生成される。この応答メッセージｔｍ２１は管理サーバ装置１８から送信され移動機１６により受信される。移動機１６では、応答メッセージｔｍ２１の受信を契機として、応答メッセージｔｍ２１内のリストファイル２００がＨＴＭＬに従って解釈され、移動機１６のユーザに対して、リストファイル２００の内容に応じたＵＩが提供される。この結果、移動機１６の表示部１６Ｃには、例えば図１０に示すようなリストページ２０１が表示される。

このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ｂが押下されるように移動機１６を操作すると、移動機１６

では、選択肢２０１Ｂに対応付けられているＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２２が生成される。この要求メッセージｔｍ２２は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２２の内容に対応して説明ファイル２０７を内包した応答メッセージｔｍ２３が生成される。この応答メッセージｔｍ２３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０７の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１４に示すような説明ページ２０８が表示される。

この説明ページ２０８を視たユーザが、説明ページ２０８内のアンカー２０８Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１３の説明ファイル２０７に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/horoscope.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２０９の送信を要求する内容の要求メッセージｔｍ２６が生成される。この要求メッセージｔｍ２６は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２６の内容に対応してＡＤＦ２０９を内包した応答メッセージｔｍ２７が生成される。この応答メッセージｔｍ２７はＩＰサーバ装置１２から送信され移動機１６により受信される。

移動機１６では、ＡＤＦ２０９の内容に基づいて第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では非

トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

次に、移動機１６では、ＡＤＦ２０９が不揮発性メモリ１６Ｄに書き込まれる。また、移動機１６では、ＡＤＦ２０９からパッケージＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１０の送信を要求する内容の要求メッセージｔｍ２８が生成される。この要求メッセージｔｍ２８は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２８の内容に対応してＪａｒファイル２１０を内包した応答メッセージｔｍ２９が生成される。この応答メッセージｔｍ２９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１０が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、第２の非トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において、第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ２０９の取得を開始する前の状態に戻る。

（３－１－３）トラステッドＪａｖａ－ＡＰソフトウェア

トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０２またはリストファイル２００の取得を試みることから始まる。説明ファイル２０２の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル２０２の取得を試みることから始まる動作についての説明を省略する。

図１９に示されるように、リストファイル２００の取得を試みることから始まる動作において、移動機１６が応答メッセージｔｍ２１を受信し、例えば図１０に示すようなリストページ２０１が表示されるまでは図１８に示す動作と同一の動作が行われる。このリストページ２０１を

視たユーザが、リストページ２０１内の選択肢２０１Ａが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ａに対応付けられているＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ３２が生成される。この要求メッセージｔｍ３２は移動機１６から送信されＩＰサーバ装置１３により受信される。

ＩＰサーバ装置１３では、この要求メッセージｔｍ３２の内容に対応して説明ファイル２０２を内包した応答メッセージｔｍ３３が生成される。この応答メッセージｔｍ３３はＩＰサーバ装置１３から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０２の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１６に示すような説明ページ２０３が表示される。

この説明ページ２０３を視たユーザが、説明ページ２０３内のアンカー２０３Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１５の説明ファイル２０２に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.main.bbb.co.jp/viewer.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２０５の送信を要求する内容の要求メッセージｔｍ３４が生成される。この要求メッセージｔｍ３４は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３４の内容に対応してＡＤＦ２０５を内包した応答メッセージｔｍ３５が生成される。この応答メッセージｔｍ３５はＩＰサーバ装置１３から送信され、ゲートウェイサーバ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。

移動機１６において、ＡＤＦ２０５は不揮発性メモリ１６Ｄに書き込まれ、ＡＤＦ２０５の内容に基づいてトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動

機１６はトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６ではトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

そして、移動機１６では、ＡＤＦ２０５に内包されているＳＤＦ－ＵＲＬ“http://www.aaa.co.jp/viewer.sdf”で特定されるＳＤＦ２０４の送信を要求する内容の要求メッセージｔｍ３６が生成される。この要求メッセージｔｍ３６は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ３６の内容に対応してＳＤＦ２０４を内包した応答メッセージｔｍ３７が生成される。この応答メッセージｔｍ３７は管理サーバ装置１８から送信されゲートウェイ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。ここで、管理サーバ装置１８とゲートウェイサーバ装置１７との間の通信路は専用線であり、ゲートウェイサーバ装置１７はセキュリティの確保された移動パケット通信網１５に直接的に接続されていることから、移動機１６に受信されるまでにＳＤＦ２０４が改竄される虞は無い。

さらに、移動機１６では、ＡＤＦ２０５に内包されている公開鍵を用いてＳＤＦ２０４の正当性が判断される。前述のように、ＡＤＦ２０５に内包されている公開鍵はＳＤＦ２０４への署名の際に用いた秘密鍵と対応していることから、管理サーバ装置１８内においてＳＤＦ２０４の内容が変更されていない限り、ＳＤＦ２０４が正当であると判断される。

ＳＤＦ２０４が正当であると判断されると、移動機１６では、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡＰＩＤとが比較される。前述のように、ＩＰサーバ装置１３におけるＡＤＦ２０５にはＳＤＦ２０４内のＡＰＩＤと一致するＡＰＩＤが記述されるように定められていることから、記述ミス等が無い限り、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡ

ＰＩＤは一致する。次いで、移動機１６では、ＳＤＦ２０４が不揮発性メモリ１６Ｄに書き込まれる。

次に、移動機１６では、ＡＤＦ２０５からパッケージＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２０６の送信を要求する内容の要求メッセージｔｍ３８が生成される。この要求メッセージｔｍ３８は移動機１６から送信されＩＰサーバ装置１３により受信される。

ＩＰサーバ装置１３では、この要求メッセージｔｍ３８の内容に対応してＪａｒファイル２０６を内包した応答メッセージｔｍ３９が生成される。この応答メッセージｔｍ３９はＩＰサーバ装置１３から送信され移動機１６により受信される。

次に、移動機１６ではＪａｒファイル２０６と所定のハッシュ関数とを用いてハッシュ値が算出され、このハッシュ値とＡＤＦ２０５に内包されているハッシュ値とが比較される。前述のように、ＡＤＦ２０５にはこのＡＤＦ２０５に対応するＪａｒファイルのハッシュ値が記述されるように定められていることから、記述ミス等がない限り、両ハッシュ値は一致する。

両ハッシュ値が一致すると、移動機１６では、Ｊａｒファイル２０６が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６においてＳＤＦ２０４が正当でないと判断された場合や、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡＰＩＤが不一致の場合、トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とＡＤＦ２０５に内包されているハッシュ値とが不一致の場合には、移動機１６の状態はＡＤＦ２０５の取得を開始する前の状態に戻る。

（３－２）Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動

次に、上述の各々のＪａｖａ－ＡＰソフトウェアが起動されている時

の移動機１６の挙動について説明する。

（３－２－１）非トラステッドＪａｖａ－ＡＰソフトウェアの挙動

上述したインストール動作により移動機１６にインストールされた非トラステッドＪａｖａ－ＡＰソフトウェア（第１の非トラステッドＪａｖａ－ＡＰソフトウェア（詰め将棋）及び第２の非トラステッドＪａｖａ－ＡＰソフトウェア（星占い）の双方を含む）が、ＪＡＭが実現された移動機１６において起動され、このソフトウェアに対応した機能（以後、非トラステッドＪａｖａ－ＡＰ）が移動機１６内に実現されたときの移動機１６の挙動について説明する。

非トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合、前述したように非トラステッドＡＰＩはあらゆるＪａｖａ－ＡＰの使用が許可されているから、この場合のＡＰＩの使用はＪＡＭにより許可されることとなる。したがって、非トラステッドＪａｖａ－ＡＰはこの非トラステッドＡＰＩを使用することができる。

また、非トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、ＪＡＭはこのＪａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄに記憶されているか否かを調べる。ここでは、そのようなＳＤＦは不揮発性メモリ１６Ｄに記憶されていないから、ＪＡＭは非トラステッドＪａｖａ－ＡＰによるこのＡＰＩの使用を禁止する。したがって、非トラステッドＪａｖａ－ＡＰはトラステッドＡＰＩを使用することができない。

（３－２－２）トラステッドＪａｖａ－ＡＰソフトウェアの挙動

移動機１６にインストールされたトラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）が、ＪＡＭが実現された移動機１６において起動され、このソフトウェアに対応した機能が移動機１６内に実現されたときの移動機１６の挙動について説明する。

トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合、前述したように、このＡＰＩの使用はＪＡＭによって当然許可される。したがって、トラステッドＪａｖａ－ＡＰはこの

非トラステッドＡＰＩを使用することができる。

トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、このＪａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄに記憶されているので、このＡＰＩの使用はＪＡＭによって許可され得るが、そのトラステッドＪａｖａ－ＡＰの挙動はＳＤＦ内のポリシー情報に依存する。以下、使用するＡＰＩ毎にその挙動について説明する。

（３－２－２－１）getPhoneList()

“getPhoneList()”はトラステッドＡＰＩであるから、このＡＰＩの使用の可否は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図４に示される通りであることから、“getPhoneList()”の使用がＪＡＭにより許可される。したがって、トラステッドＪａｖａ－ＡＰ（電話帳ビューワ）は“getPhoneList()”を使用することができる。つまり、このトラステッドＪａｖａ－ＡＰは電話帳データを読み出すことができる。

（３－２－２－２）getCallHistory()

“getCallHistory()”はトラステッドＡＰＩであるから、このＡＰＩの使用の可否はＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図４に示される通りであることから、“getCallHistory()”の使用がＪＡＭにより禁止される。したがって、トラステッドＪａｖａ－ＡＰ（電話帳ビューワ）は“getCallHistory()”を使用することができない。つまり、このトラステッドＪａｖａ－ＡＰは発着信履歴データを読み出すことができない。

（３－３）トラステッドＪａｖａ－ＡＰソフトウェアの有効期限更新時の動作

次に、トラステッドＪａｖａ－ＡＰソフトウェアの有効期限を更新する動作例について説明する。以下の説明においては、図９において、管理サーバ装置１８内においてＳＤＦ２０４がＳＤＦ２０４ａに更新さ

れているものとする。ただし、その更新内容は、有効期限が“２００２年１０月１日午前１０時”から“２００３年1月１日午前１０時”に変更されたということのみであり、ＳＤＦ２０４とＳＤＦ２０４ａの記憶位置やそのファイル名、署名に用いた秘密鍵等は一切変更されていないものとする。

移動機１６は、計時部１６Ｈによって計時される現在日時と、今までに取得した全てのＳＤＦに内包されている複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している。ここで、計時部１６Ｈによって計時される現在日時が２００２年１０月１日午前１０時となったとき、ＡＰＩＤ“0001”に対応するトラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）の有効期限が到来することとなり、これによって、図２０に示す動作が開始される

まず、移動機１６は、図２１に示すように、有効期限が到来したトラステッドＪａｖａ－ＡＰソフトウェアの名称“電話帳ビューワ”とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部１６ｃに表示してユーザの操作があるまで待機する。

ここで、ユーザが有効期限を更新することを指示する操作を行うと、移動機１６はこの指示内容を解釈し、ＡＰＩＤ“0001”を内包したＡＤＦに内包されているＳＤＦ－ＵＲＬ（“http://www.aaa.co.jp/viewer.sdf”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ４１を生成する。この要求メッセージｔｍ４１は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ４１の内容に対応してＳＤＦ２０４ａを内包した応答メッセージｔｍ４２が生成される。この応答メッセージｔｍ４２は管理サーバ装置１８から送信され移動機１６により受信される。

一方、移動機１６は、上記ＳＤＦ－ＵＲＬを用いてＳＤＦ２０４ａを取得できたか否かを判断する。ここでは取得に成功することを想定して

いるので処理は次に進み、移動機１６は、ＳＤＦ２０４ａの署名を、既に取得しているＡＤＦ２０５に内包されている公開鍵を用いて検証し（復号し）、このＳＤＦ２０４ａの正当性を判断する。正当性が確認されると（ステップＳ３５；Ｙｅｓ）、移動機１６は、ＳＤＦ２０４ａから抽出したＡＰＩＤと既に取得済みのＡＤＦ２０５に内包されていたＡＰＩＤとを比較し、両者が一致するか否かを判定する。

ここでは両者が一致するはずなので、移動機１６は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０３をＳＤＦ２０４ａで上書きし、これにより、トラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）の有効期限が“２００２年１０月１日午前１０時”から“２００３年１月１日午前１０時”に更新される。

なお、ユーザの操作により有効期限を更新しないと判断された場合、ＳＤＦを取得できなかった場合、ＳＤＦが正当でないと判断した場合、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合、ＪＡＭは、有効期限を更新しない旨をユーザに通知するとともに、移動機１６の状態をＳＤＦ２０３ａを取得する以前の状態に戻す。

（３－４）トラステッドＪａｖａ－ＡＰソフトウェアの変更後の動作

次に、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰがトラステッドＪａｖａ－ＡＰソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、トラステッドＪａｖａ－ＡＰソフトウェアの改善等を目的としたＪａｒファイル２０６の内容の変更と、ＩＰサーバ装置１３の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰは、図２２に示すように、変更後のＪａｒファイル２０６（以後、Ｊａｒファイル２１５）をＩＰサーバ装置１４の不揮発性メモリ１４Ａに記憶させ、このＪａｒファイル２１５に対応するようにＡＤＦ２０５の内容を変更してＡＤＦ２１６としている。変更後のトラステッドＪａｖａ－ＡＰソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置

１８を管理する通信事業者が行うべき作業は存在しない。つまり、通信事業者はリストファイル２００やＳＤＦ２０４を変更する必要はない。

このような変更の後のトラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、図２３に示す通りとなる。この図に示す動作が図１９に示す動作と相違し始めるのは、移動機１６がＪａｒファイルを要求する時点からである。なお、両図において、応答メッセージｔｍ４７は応答メッセージｔｍ３７、要求メッセージｔｍ４８は要求メッセージｔｍ３８、応答メッセージｔｍ４９は応答メッセージｔｍ３９に対応している。

即ち、図２３において図１９に示す動作と本質的に異なるのは、ＡＤＦ２１６およびＪａｒファイル２１５が処理の対象となる点と、ＡＤＦ２１６に内包されているパッケージＵＲＬ（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるＪａｒファイル２１５の送信を要求する内容の要求メッセージｔｍ４８が移動機１６にて生成される点と、この要求メッセージｔｍ４８が移動機１６から送信されＩＰサーバ装置１４により受信される点と、ＩＰサーバ装置１４においてＪａｒファイル２１５を内包した応答メッセージｔｍ４９が生成される点と、この応答メッセージｔｍ４９がＩＰサーバ装置１４から送信され移動機１６により受信される点のみである。

以上説明したように、移動機１６においては、ダウンロードしたＳＤＦに含まれるポリシー情報の内容に応じた挙動がこのＳＤＦに対応するトラステッドＪａｖａ－ＡＰソフトウェアに許可され、ポリシー情報の内容に含まれていない挙動は許可されない。このポリシー情報は管理サーバ装置１８からセキュリティが確保された上で移動機１６へ送信されるから、ポリシー情報が第三者により改竄される虞もなく、これにより、トラステッドＪａｖａ－ＡＰの信頼性が確保される。また、ユーザから視れば、従来通りの非トラステッドＪａｖａ－ＡＰの他に、上記のような、より自由な挙動が許可されたトラステッドＪａｖａ－ＡＰを利用可能となり、非常に便利である。

なお、上述の配信システムにおいては、移動機１６に対し、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各種ファイルの配信を行っていたが、このような順序で配信することにより、以下のような効果が生ずる。

既に説明したように、Ｊａｖａ－ＡＰソフトウェア（ＡＤＦ及びＪａｒファイル）はＩＰによって設計・作成され、各々のＩＰがインターネット上に開設している専用サイト（図１のＩＰサーバ装置１２～１４）において、一般ユーザに公開されている。従って、ユーザはまず、ＩＰの専用サイトにアクセスし、そこで、様々なＪａｖａ－ＡＰソフトウェアの解説ページを参照してそのソフトウェアをダウンロードをするか否かを判断するのが普通である。そして、ユーザはＪａｖａ－ＡＰソフトウェアをダウンロードしようと判断すると、そのダウンロード処理を指示する操作を行う必要があるが、そのために上記の解説ページには次にダウンロードすべきファイルのＵＲＬがアンカータグによって埋め込まれているのが普通である。このとき、ＩＰの立場から視れば、解説ページにＡＤＦのＵＲＬを埋め込むのが最も手間がかからない。なぜなら、ＡＤＦはＩＰの管理下にあるので、そのＡＤＦのＵＲＬはＩＰによって常に把握できているからである。これに対し、解説ページにＳＤＦのＵＲＬを埋め込むとなると、ＩＰは通信事業者に問い合わせをする等して、ＵＲＬの正誤の確認処理を絶えず欠かさないようにしなければならない。よって、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各種ファイルの配信を行うことは非常に有意義である。

また、上記の順序は、エヌティティドコモ社のｉモード（登録商標）において現在実施されているＪａｖａ－ＡＰソフトウェアのバージョンアップ処理を考慮した場合にも利点がある。現状のｉモードのサービス仕様においては、ユーザによってバージョンアップを要求する操作がなされると、移動機は、まず、ＡＤＦに記述された内容を参照し、ＡＤＦに記述されたパッケージＵＲＬに基づいて、バージョンアップ後のＪａｒファイルを取得するようになっている。即ち、バージョンアップ時には、まずＡＤＦを参照してから、その後にダウンロード処理に移行す

るようになっている。この点を考慮すると、本実施形態の配信システムにおけるバージョンアップ時においても、まずＡＤＦを参照し、そのＡＤＦに記述されているＳＤＦ－ＵＲＬに基づいてＳＤＦを取得した後、Ｊａｒファイルを取得するというように、まずＡＤＦの参照から一連の処理を開始すると、それ以降は、ＳＤＦ→Ｊａｒファイルという通常のダウンロードと同じ流れで処理を行うことができ、現状のサービス仕様をあまり変更しないで済む。これに対し、仮にＳＤＦ、ＡＤＦ、Ｊａｒファイルという順序で各種ファイルをダウンロードすることが定義付けられている場合、バージョンアップしようとした場合、ＡＤＦを参照からダウンロード処理を開始すると、ＳＤＦを取得することなくＪａｒファイルの取得処理にまで至ってしまう。ＳＤＦは、バージョンアップ時に書き換えられることは十分にあり得るので、ＳＤＦが無いとセキュリティ上で不都合が生ずるおそれがある。以上のような観点からも、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各種ファイルの配信を行うことは有意義である。

（３）変形例

本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてＳＤＦとＡＤＦの作成者との対応関係の正当性を確認するようにした。しかし、これに限らず、ＳＤＦとＡＤＦの作成者との対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、ＳＤＦに公開鍵を内包させず、ＩＰサーバ装置においてはＡＤＦに対する秘密鍵を用いた署名を行わず、かつ移動機においてはこの確認処理を省略する、という形態とし、移動機およびＩＰサーバ装置における処理量や、移動機と管理サーバ装置およびＩＰサーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、Ｊａｒファイルのハッシュ値をこのＪａｒファイルに対応するＡＤＦに内包させる一方、移動機においてＪａｒファイルのハッシュ値を生成し、これら両者を比較してＪａｒファイルとＡＤＦとの対応関係の正当性を確認するようにしていた。しかし、これに限らず、ＪａｒファイルとＡＤＦとの対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、ＡＤＦにハッシュ値を内包させずにこの確認処理を省略する形態とし、移動機およびＩＰサーバ装置における処理量や移動機とＩＰサーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、トラステッドＪａｖａ－ＡＰに固有のＡＰＩＤを使用してＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドＪａｖａ－ＡＰを提供する情報提供事業者に固有のＣＩＤを用いてＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、ＡＰＩＤやＣＩＤを用いた判定を省略するようにしてもよい。

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、ＩＰアドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、ＡＤＦに内包されているＳＤＦ－ＵＲＬのうちのドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、ＳＤＦを正当と認める態様としてもよい。この場合、予め設定された文字列と異なるときは、移動機１６は、ＳＤＦ取得に失敗した旨を表示し、管理サーバ１８にＳＤＦを要求せずに処理を終了することとなる。

また、この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のＲＯＭまたは不揮発性メモリに予

め格納されることになる。ＲＯＭに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

また、上述した配信システムでは、ＳＤＦの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がＳＤＦを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、ＳＤＦを暗号化した後に配信し、移動機においてＳＤＦを復号するようにすれば、ある程度のセキュリティを確保してＳＤＦを配信することができる。

上述した配信システムでは、ＨＴＴＰに従ってファイルを送受するようにしたが、ＨＴＴＰＳを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

また、上述した配信システムにおいて、信頼できる機関がＩＰとなってよいこと、すなわち、管理サーバ装置がＩＰサーバ装置を兼ねるようにしてもよいことは言うまでもない。

さらに、上述した配信システムでは、Ｊａｖａ－ＡＰによる利用を制限する対象としてＡＰＩを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、ＬＥＤ（Light Emitting Diode）等の移動機が備え得るものや、移動機と共働し得るＵＩＭ（User Identity Module）やＳＩＭ（Subscriber Identity Module）等の外部機器なども挙げられる。

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

次にソフトウェア資源について説明する。ソフトウェア資源としては、ＡＰＩやクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Ｗｅｂブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

ところで、Ｊａｖａ－ＡＰによるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限することにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Ｊａｖａ－ＡＰのうちのトラステッドＪａｖａ－ＡＰについてのみ、自他のＪａｖａ－ＡＰの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの２つの利用形態（利用の種類）があるから、非トラステッドＪａｖａ－ＡＰには読み出しでしか利用されないが、トラステッドＪａｖａ－ＡＰには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、１つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するＪａｖａ－ＡＰが起動されている間にＷｅｂブラウザ等が起動された場合、このＪａｖａ－ＡＰが「パケット伝送路の利用を排他的に行う」ことを許可されていないＪａｖａ－ＡＰであればＷｅｂブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているＪａｖａ－ＡＰであればパケット伝送路を占有して使用することができる、といった制御が可能となる。

さらに、この例を変形することで、ある種のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはパ

ケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

また、上述の配信システムでは、Ｊａｖａ－ＡＰの実行時にＪａｖａ－ＡＰの挙動を制限するようにしたが、ＩＰサーバ装置に格納されているＪａｒファイルにポリシー情報を内包させ、Ｊａｒファイルのダウンロード時に、移動機において、このポリシー情報とＳＤＦ中とのポリシー情報とを比較し、両者が一致しない場合には、このＪａｒファイルに対応するＪａｖａ－ＡＰを起動できないように、あるいはこのＪａｒファイルを含むＪａｖａ－ＡＰソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

通信事業者の公開鍵は、ＩＰサーバ装置１２～１４からＡＤＦに含めて移動機１６に提供されるようになっていたが、これに限らず、予め移動機に格納されていてもよい。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、ＲＯＭに書き込んだ後に移動機を販売する方法などが考えられる。

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

上述の配信システムでは、トラステッドＪａｖａ－ＡＰソフトウェアの有効期限が到来したタイミングで、その有効期限を更新するための処理を開始していた。しかし、更新タイミングは上記のものに限らず、ユーザが所望する恣意的なタイミングや、毎月末１回等の定期的なタイミングというように、様々な態様を採用し得る。

また、有効期限の設定の仕方は、既に説明したように日時によって設定してもよいが、この他にも、例えばトラステッドＪａｖａ－ＡＰソフトウェアのダウンロード時からの期間（例えばダウンロードしてから１ヶ月のみ使用可能というような場合）によって設定してもよいし、トラステッドＪａｖａ－ＡＰソフトウェアの実行回数や実行期間によって設定してもよい。要するに、有効期限とは、Ｊａｖａ－ＡＰソフトウェアを無制限には実行できないようにその上限を定めた情報であればどのようなものであってもよい。

例えば実行回数で有効期限を設定した場合、トラステッドＪａｖａ－ＡＰソフトウェアの起動時にＪＡＭはＳＤＦ内のポリシー情報を参照するようになっているので、その参照回数をトラステッドＪａｖａ－ＡＰソフトウェアの実行回数としてカウントしてもよい。そして、カウントした実行回数が予め定められた数に達すると、その更新処理に移行すればよい。

また、トラステッドＪａｖａ－ＡＰソフトウェアが実行されている期間を累積してカウントするような手段（例えばそのトラステッドＪａｖａ－ＡＰソフトウェア内にサブルーチンとして記述する等の手段）を備えていれば、実行期間によって有効期限を設定した場合にも対応できる。そして、カウントした実行期間が予め定められた時間に達すると、その更新処理に移行すればよい。

なお、上述の配信システムの説明では「トラステッドＪａｖａ－ＡＰソフトウェアの有効期限」という表現を用いていたが、より厳密には、Ｊａｒファイルそのものの有効期限であってもよいし、ＳＤＦそのものの有効期限であってもよいし、その両者の有効期限であってもよいことはもちろんである。

また、上述の配信システムでは、有効期限が到来してもそれを更新できない場合、その有効期限が到来したトラステッドＪａｖａ－ＡＰソフトウェアを実行禁止となっていたが、これに限らず、その有効期限経過時にトラステッドＪａｖａ－ＡＰソフトウェアから非トラステッドＪ

ａｖａ－ＡＰソフトウェアに遷移させてもよい。即ち、有効期限が到来したＪａｖａ－ＡＰソフトウェアは、非Ｊａｖａ－ＡＰソフトウェアであるとみなされ、その遷移後は、非トラステッドＪａｖａ－ＡＰソフトウェアとしての、より厳しい挙動を制限を受けることとなる。

また、任意のトラステッドＪａｖａ－ＡＰソフトウェアのＳＤＦを失効させることができるように、上記実施形態を変形してもよい。

この変形例において、管理サーバは、上記実施形態と同様、各種のＪａｖａ－ＡＰソフトウェアのＳＤＦを記憶するための記憶部を有している。管理サーバの制御部は、通信部により各ＳＤＦを受信し、あるいは記憶媒体に格納されたＳＤＦを受け取ったとき、この記憶部に格納する。

また、管理サーバには、任意のトラステッドＪａｖａ－ＡＰソフトウェアについて、そのＳＤＦを失効させる旨のコマンドが入力され得る。このコマンドは、失効させるべきＳＤＦが帰属するトラステッドＪａｖａ－ＡＰソフトウェアのＡＰＩＤを含んでいる。このようなコマンドは、オペレータにより管理サーバの入力部に入力され、あるいは該当するＩＰサーバからネットワークを介して管理サーバ宛てに送信され、管理サーバの通信部によって受信される。管理サーバの制御部は、このコマンドを入力部あるいは通信部を介して受け取ると、コマンド中のＡＰＩＤにより特定されるＳＤＦが失効した旨の情報を記憶部に格納する。これにより、以後、管理サーバでは、このＳＤＦの公開が停止され、このＳＤＦを利用したＪａｖａ－ＡＰソフトウェアのダウンロードが不可能になる。

ところで、あるトラステッドＪａｖａ－ＡＰソフトウェアのＳＤＦが、ある端末装置に配信され、その後、そのＳＤＦが失効するような場合も考えられる。この場合、既に配信済みのＳＤＦがＳＤＦとして機能しないようにするべきである。そこで、次のような方法が考えられる。すなわち、端末装置がＳＤＦの有効性を例えば一定時間間隔で管理サーバに問い合わせ、ＳＤＦが失効している旨の応答が管理サーバから返ってき

たときにはそれ以降のＳＤＦの使用を禁止するのである。ここで、ＳＤＦが失効になった後、トラステッドＪａｖａ－ＡＰソフトウェアが実行される回数を減らすためには、問い合わせの時間間隔を短くするのが有効である。しかし、そのようなことを全端末装置について一律に行うと、トラヒックが膨大になりユーザが負担する通信費もかさむ。一方、端末装置のユーザの中には、頻繁にトラステッドＪａｖａ－ＡＰソフトウェアの実行を指示する人もいれば、たまにしか実行を指示しない人もいるので、後者の人のためにトラヒックおよび通信費を増やすのは得策ではない。

この問題を解決するため、本変形例では次のような処理が行われる。まず、管理サーバ装置は、ＳＤＦを通信部により端末装置に送信する際、頻度データＮと間隔データＴを含ませる。ここで、頻度データＮは、トラステッドＪａｖａ－ＡＰソフトウェアの実行回数がＮの整数倍を越える毎にＳＤＦの有効性についての問い合わせを送信することを指示するデータである。また、間隔データＴは、トラステッドＪａｖａ－ＡＰソフトウェア実行終了後、次にＪａｖａ－ＡＰソフトウェアの実行が開始される前に、時間Ｔが経過したとき、ＳＤＦの有効性についての問い合わせを送信することを指示するデータである。

端末装置は、あるＳＤＦを受信した場合、そのＳＤＦ内の頻度データＮおよび間隔データＴに従って、そのＳＤＦの有効性についての問い合わせを管理サーバ装置に送信する。図２４には、１つのＳＤＦについてこのような処理を行うための制御部の構成が示されている。端末装置が複数のＳＤＦを記憶している場合には、図２４に示すものが、これと同数だけ制御部内に用意されると考えて良い。なお、図２４において符号５０１～５０４によって示される要素は制御部を構成する回路あるいは制御部によって実行されるルーチンを表している。

まず、端末装置の制御部は、ＳＤＦを受信すると、図２４に示す回路ないしルーチンをそのＳＤＦのために活性化する。そして、ＳＤＦから頻度データＮと間隔データＴを取り出し、頻度データＮを除算器５０２

に、間隔データＴをタイマ５０３に設定する。

カウンタ５０１は、ＳＤＦに対応したトラステッドＪａｖａ－ＡＰソフトウェアが起動される都度、１ずつカウント値を増す。除算器５０２は、カウンタ５０１のカウント値、即ちトラステッドＪａｖａ－ＡＰソフトウェアの起動回数を頻度データＮによって除算し、その除算結果の余りが１になったとき、信号“１”を出力する。

タイマ５０３は、具体的にはダウンカウンタである。トラステッドＪａｖａ－ＡＰソフトウェアが起動されると、間隔データＴがカウント値の初期値として５０３に書き込まれる。その後、タイマ５０３は、所定周波数のクロックに同期して、ダウンカウントを進める。そして、Ｔ相当の時間が経過し、タイムアウトになると、タイマ５０３は信号“１”を出力する。タイムアウト前にトラステッドＪａｖａ－ＡＰソフトウェアが再起動されると、間隔データＴがタイマ５０３にセットされ、その時点から新たなダウンカウントが始まる。

ＯＲゲート５０４は、除算器５０２またはタイマ５０３から信号“１”が出力されると、ＳＤＦの有効性の問い合わせを指示する信号を発生する。

図２５は、以上説明した動作を示すタイムチャートである。同図に示すとおり、頻度データＮが与えられることにより、ＯＲゲート５０４はＮ＋１回目、２Ｎ＋１回目という具合に、ＳＤＦの有効性の問い合わせを指示する信号を発生する。制御部は、この信号が発生したとき、ＳＤＦの有効性についての問い合わせを通信部により管理サーバ装置に送る。この問い合わせは、その対象であるＳＤＦを特定するＡＰＩＤを含んでいる。管理サーバの制御部は、この問い合わせを通信部により受信すると、記憶部を参照することにより、問い合わせ中のＡＰＩＤにより特定されるＳＤＦが有効であるか失効しているかを調べ、その結果を通信部により端末装置に回答する。端末装置の制御部は、問い合わせを行ったＳＤＦが失効している旨の回答を通信部により受け取った場合、そのＳＤＦに対応したＪａｖａ－ＡＰソフトウェアが起動できないよう

制御を行う。

また、図２５に示す例では、２回目にトラステッドＪａｖａ－ＡＰソフトウェアが実行された後、３回目の実行の前に、経過時間がＴを越えたため、ＳＤＦの有効性の問い合わせを指示する信号が発生している。この場合も、上記と同様な問い合わせ、管理サーバからの応答、応答に応じた端末装置側の動作が行われる。

以上説明した本変形例の利点は次の点にある。

まず、頻繁にトラステッドＪａｖａ－ＡＰソフトウェアを使用する人の場合、間隔データＴに基づく問い合わせ発生制御だけを行うと、常にタイムアウトになる前にトラステッドＪａｖａ－ＡＰソフトウェアが起動されるため、問い合わせが行われない。従って、このようなユーザのためには、起動回数がＮを越えたときに問い合わせるという方法が有効である。

一方、トラステッドＪａｖａ－ＡＰソフトウェアをたまにしか使わない人の場合、なかなか起動回数がＮを越えないので、タイムリーにＳＤＦを失効させることができない。従って、このようなユーザのためには、起動後の経過時間がＴを越えたときに問い合わせるという方法が有効である。

本変形例は、これら両方法を並列使用するので、両方のタイプの人に有効である。

請求の範囲

1．アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、

前記端末装置が、前記配信システムから送信されてくるアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信された前記アプリケーション記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程と

を有する配信方法。

2．ネットワーク内の装置との通信を行うための通信部と、

記憶部と、

制御部とを具備し、

前記制御部は、

（ａ）アプリケーションを実現するためのソフトウェアを内包した実体ファイルの格納位置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルの格納位置を示す情報を含んだ第１の配信要求を前記通信部により前記ネットワーク内の配信システムに送信することにより、前記配信システムにおける情報提供サーバ装置に格納されたアプリケーション記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

（ｂ）前記配信システムから受信されたアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を示す情報を含んだ第２の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける管理サーバ装置に記憶されたセキュリティ記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

（ｃ）前記配信システムから受信されたアプリケーション記述ファイルに内包されている実体ファイルの格納位置を示す情報を含む第３の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける情報提供サーバに格納された実体ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

（ｄ）前記記憶部に記憶された実体ファイルに含まれるソフトウェアの実行が指示された場合に、前記記憶部に記憶された該実体ファイルに対応したセキュリティ記述ファイルに含まれる権限情報に従い、該ソフトウェアの実行により実現されるアプリケーションの挙動を制限する手段と

を有する端末装置。

３．前記配信システムは、前記セキュリティ記述ファイルを暗号化して

前記端末装置に送信することによってセキュリティを確保しており、

前記制御部は、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する手段を具備する請求項２に記載の端末装置。

４．前記制御部は、前記通信部により、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを受信する請求項２に記載の端末装置。

５．前記制御部は、暗号化通信により前記セキュリティ記述ファイルを受信する請求項２に記載の端末装置。

６．前記制御部は、前記通信部により、移動通信網および専用線を介して前記セキュリティ記述ファイルを受信する請求項２に記載の端末装置。

７．前記制御部は、移動通信網を介した暗号化通信により前記セキュリティ記述ファイルを受信する請求項２に記載の端末装置。

８．前記制御部におけるアプリケーションの挙動を制限する手段は、前記セキュリティ記述ファイルに内包された権限情報に基づき、資源の利用を制限する請求項２に記載の端末装置。

９．前記資源は前記端末装置内部のハードウェア資源である請求項８に記載の端末装置。

１０．前記資源は前記端末装置外部の、当該端末装置が使用可能なハードウェア資源である請求項８に記載の端末装置。

１１．前記資源は前記端末装置内部のソフトウェア資源である請求項８に記載の端末装置。

１２．前記資源は前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源である請求項８に記載の端末装置。

１３．前記資源は、前記端末装置が使用可能なネットワーク資源である請求項８に記載の端末装置。

１４．前記制御部におけるアプリケーションの挙動を制限する手段は、前記権限情報に基づき資源の利用の種類を判断する請求項２に記載の端末装置。

１５．前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、

前記制御部は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する請求項２に記載の端末装置。

１６．前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記制御部は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包さ

れたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する請求項２に記載の端末装置。

１７．前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記制御部は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する請求項２に記載の端末装置。

１８．前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、前記制御部は、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから当該セキュリティ記述ファイルが時系列的に繰り返し受信し、繰り返し受信される前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する手段を具備する請求項２に記載の端末装置。

１９．前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてきた場合にのみ、前記アプリケーションの有効期限を更新する請求項１８に記載の端末装置。

２０．前記端末装置は移動機である請求項２に記載の端末装置。

２１．アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述

されたアプリケーション記述ファイルを格納した１または複数のサーバ装置とを有し、

前記１または複数のサーバ装置のうち前記セキュリティ記述ファイルを格納するサーバ装置は、セキュリティ記述ファイルを管理する権限の与えられた管理サーバ装置であり、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送する手段を有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する

配信システム。

２２．通信部と、

記憶部と、

（ａ）ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを前記記憶部に書き込む処理と、

（ｂ）前記セキュリティ記述ファイルの有効性に関する情報を前記記憶部に書き込む処理と、

（ｃ）前記セキュリティ記述ファイルの有効性に関する問い合わせが前記通信部により端末装置から受信されたとき、当該セキュリティ記述ファイルの有効性に関する情報を前記記憶部から読み出し、前記通信部により前記端末装置に通知する処理と

を行う制御部とを具備する管理サーバ装置。

２３．通信部と、

記憶部と、

（ａ）ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイ

ルを前記通信部により管理サーバから受信し、前記記憶手段に書き込む処理と、

（ｂ）前記記憶手段に格納されたセキュリティ記述ファイルの有効性に関する問い合わせを前記通信部により前記管理サーバ装置に繰り返し送信する処理と、

（ｃ）前記セキュリティ記述ファイルが失効している旨の回答が前記通信部により前記管理サーバ装置から受信された場合に、当該セキュリティ記述フィルに対応付けられた実体ファイルを起動不能状態にする処理と

を実行する制御部とを具備する端末装置。

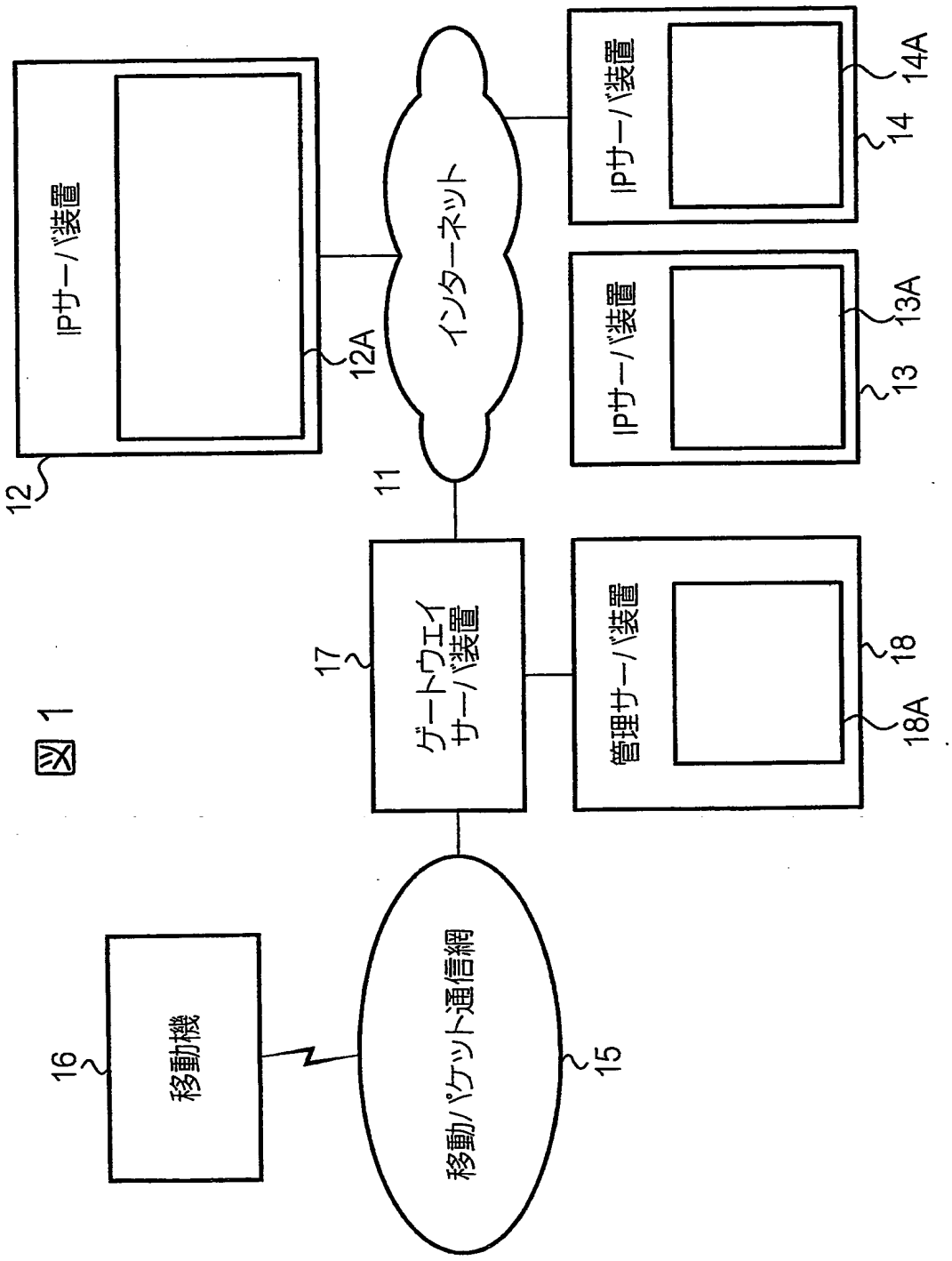

IPサーバ装置
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
13
13A
ゲートウエイ
サーバ装置
17
管理サーバ装置
18
18A
移動機
16
移動パケット通信網
15

図 1

図 2

APID	ハッシュ値	パッケージURL	•••	SDF-URL	公開鍵

図 3

APID	ポリシー情報	有効期限

図 4

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

図 5

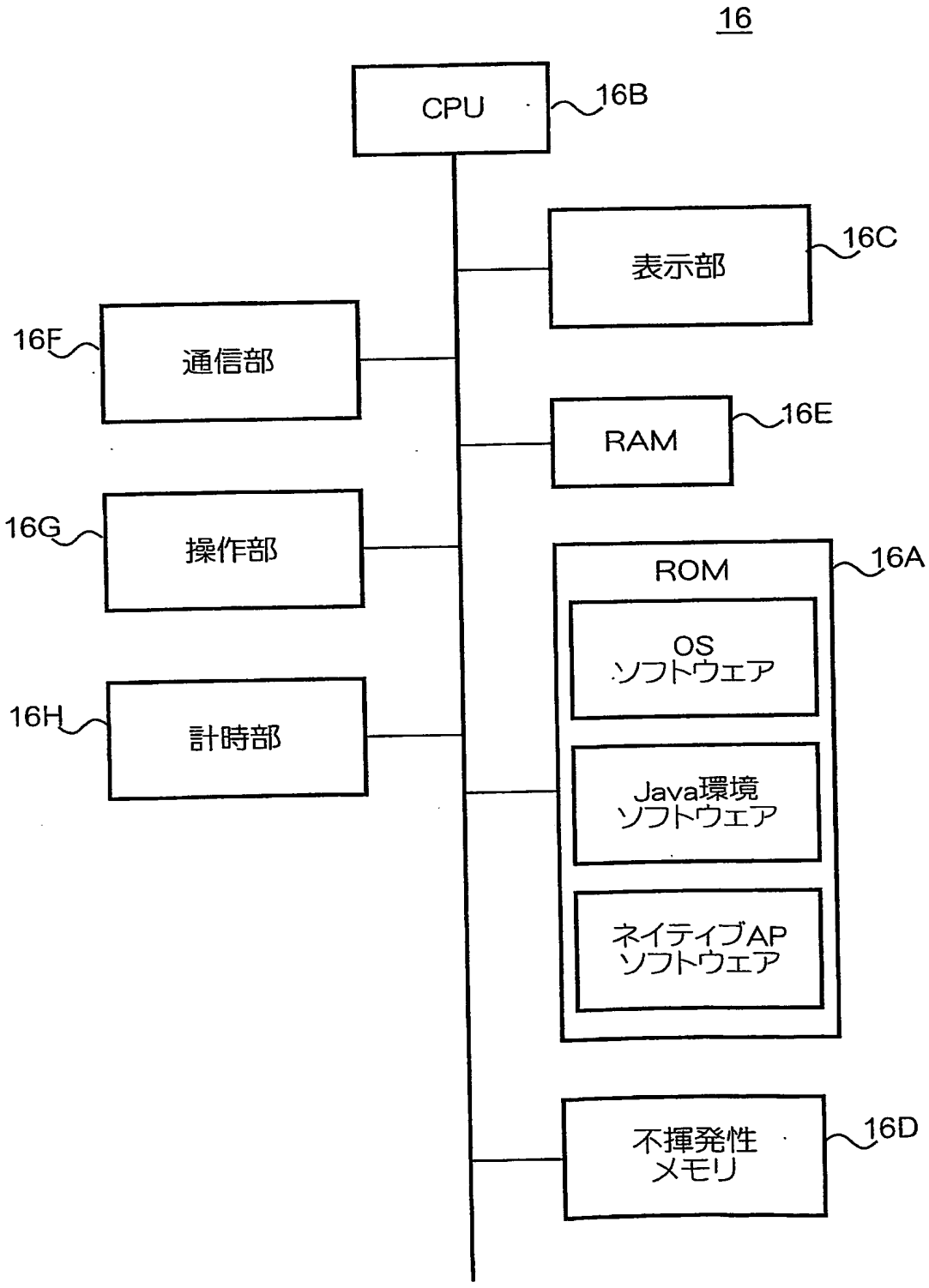

16
CPU
16B
表示部
16C
16F
通信部
RAM
16E
16G
操作部
ROM
16A
OS
ソフトウェア
16H
計時部
Java環境
ソフトウェア
ネイティブAP
ソフトウェア
不揮発性
メモリ
16D

図6

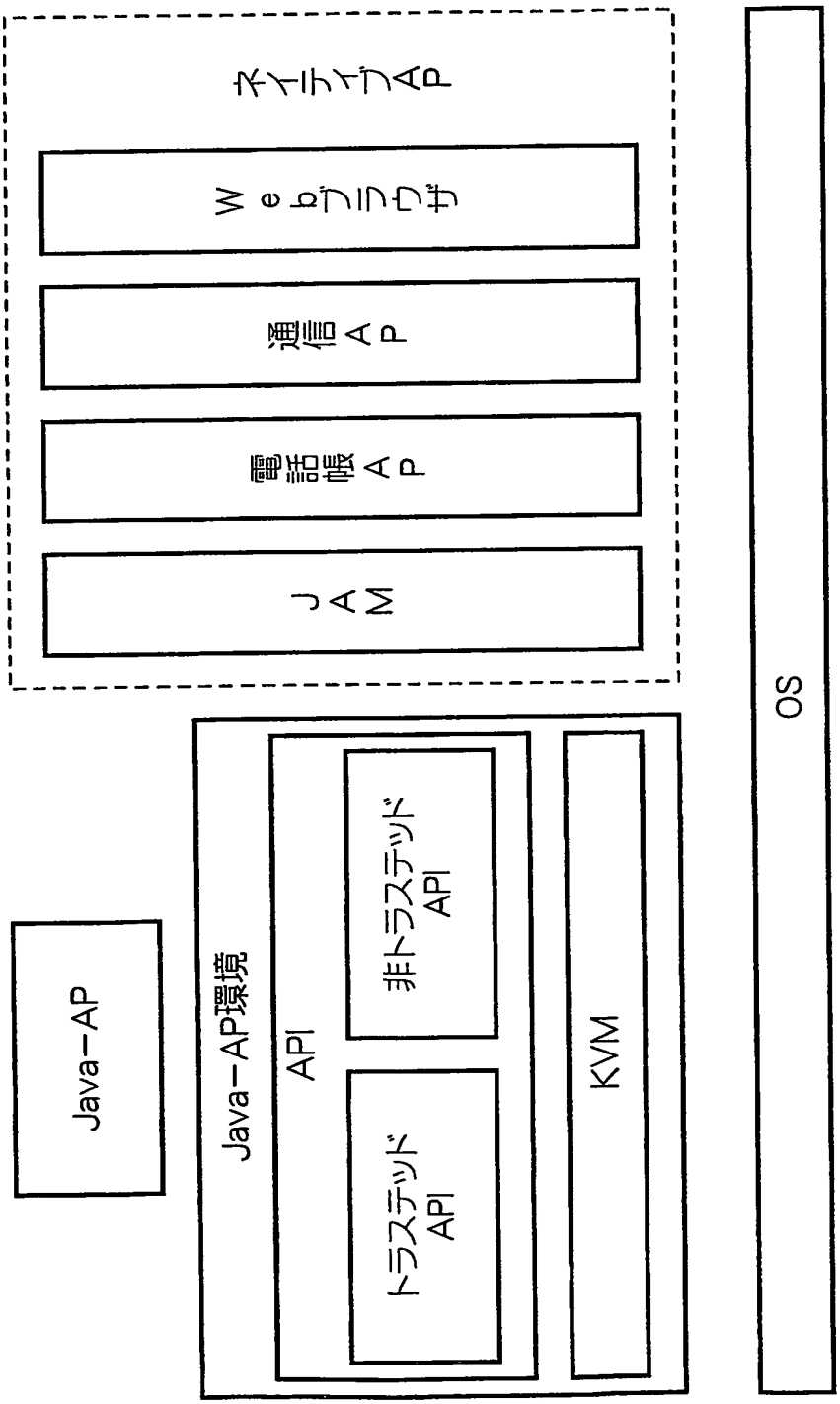

ネイティブAP
Webブラウザ
通信AP
書誌情報AP
JAM
OS
Java−AP
Java−AP環境
API
非トラステッドAPI
トラステッドAPI
KVM

図 7

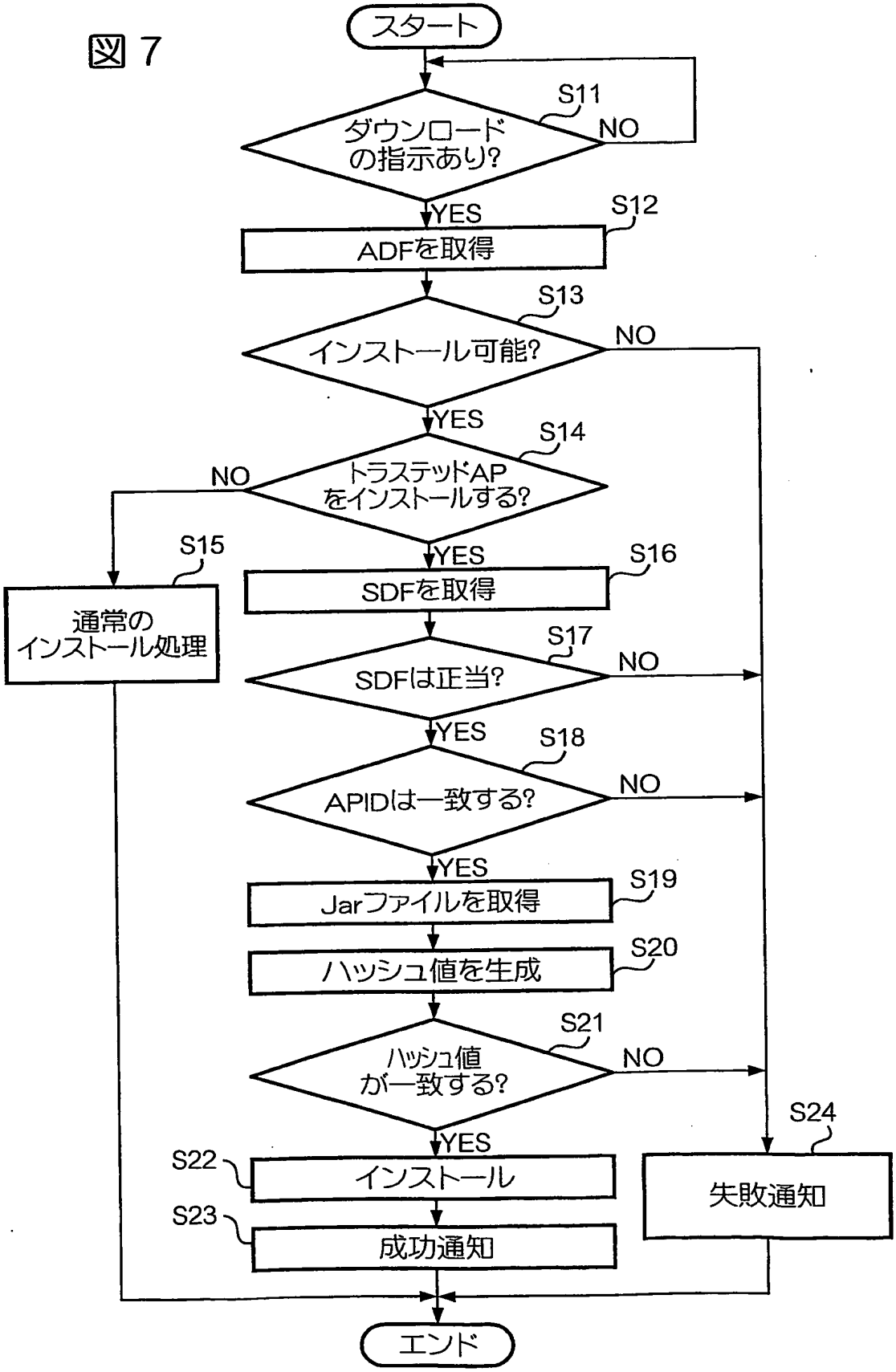
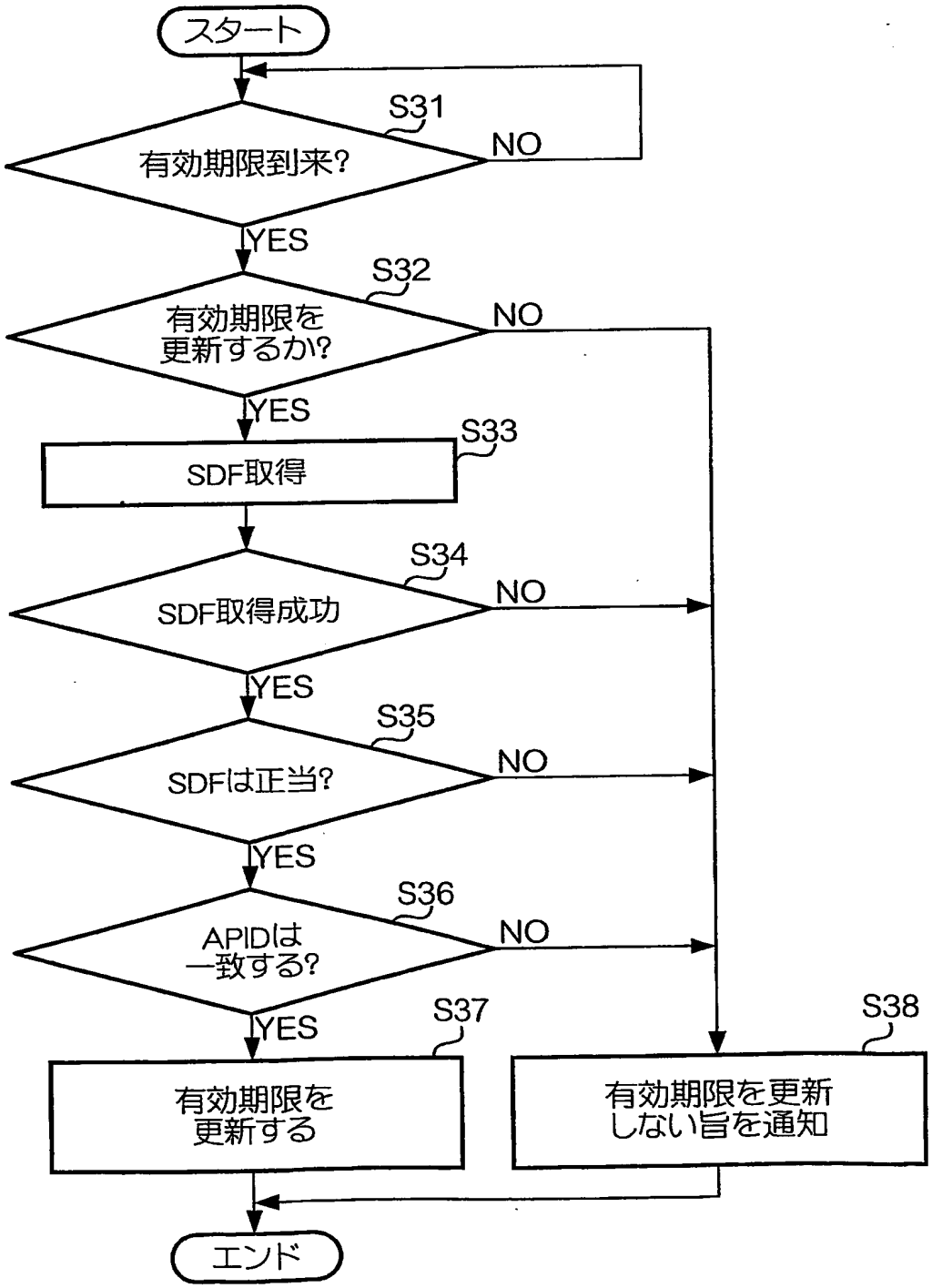

スタート
S11
ダウンロードの指示あり?
NO
YES
S12
ADFを取得
S13
インストール可能?
NO
YES
S14
トラステッドAPをインストールする?
NO
YES
S15
通常のインストール処理
S16
SDFを取得
S17
SDFは正当?
NO
YES
S18
APIDは一致する?
NO
YES
S19
Jarファイルを取得
S20
ハッシュ値を生成
S21
ハッシュ値が一致する?
NO
YES
S22
インストール
S23
成功通知
S24
失敗通知
エンド

図 8


スタート
S31
有効期限到来?
NO
YES
S32
有効期限を
更新するか?
NO
YES
S33
SDF取得
S34
SDF取得成功
NO
YES
S35
SDFは正当?
NO
YES
S36
APIDは
一致する?
NO
YES
S37
有効期限を
更新する
S38
有効期限を更新
しない旨を通知
エンド

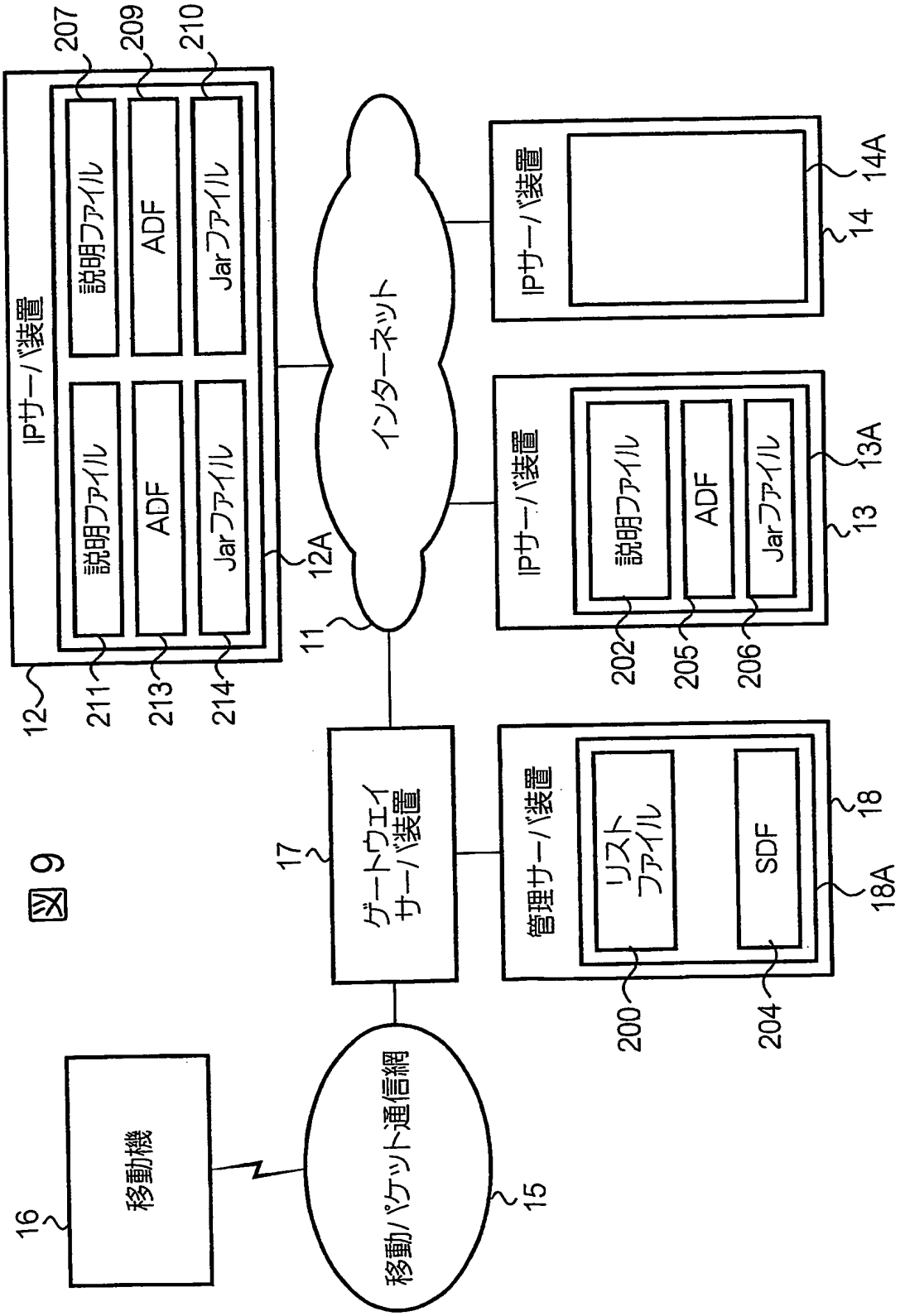

IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
説明ファイル
ADF
Jarファイル
13
13A
202
205
206
ゲートウェイ
サーバ装置
17
管理サーバ装置
リスト
ファイル
SDF
18
18A
200
204
移動パケット通信網
15
移動機
16

図 9

図 10

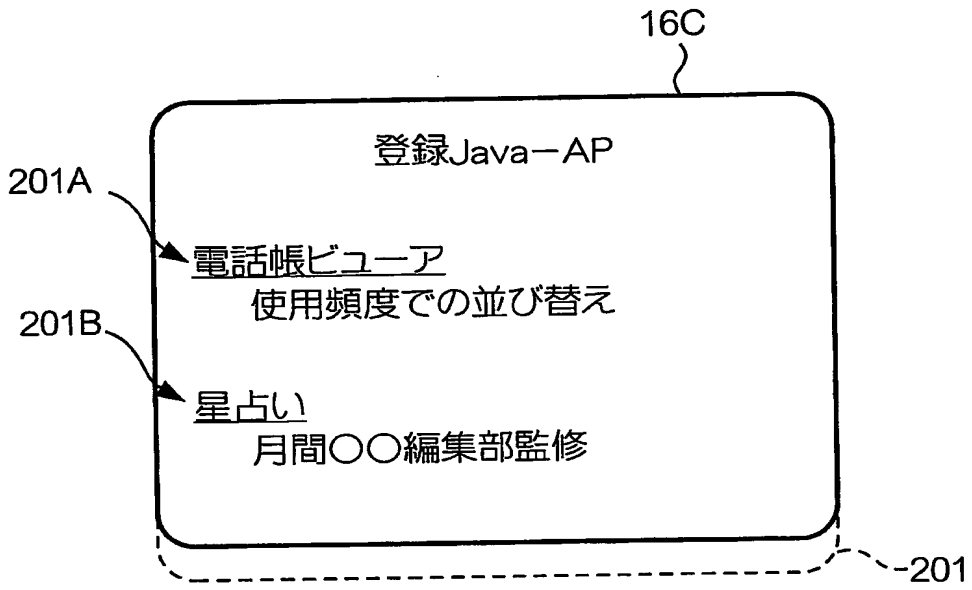


図 11

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/shogi.jam>
詰め将棋
</OBJECT>
～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。

図 12

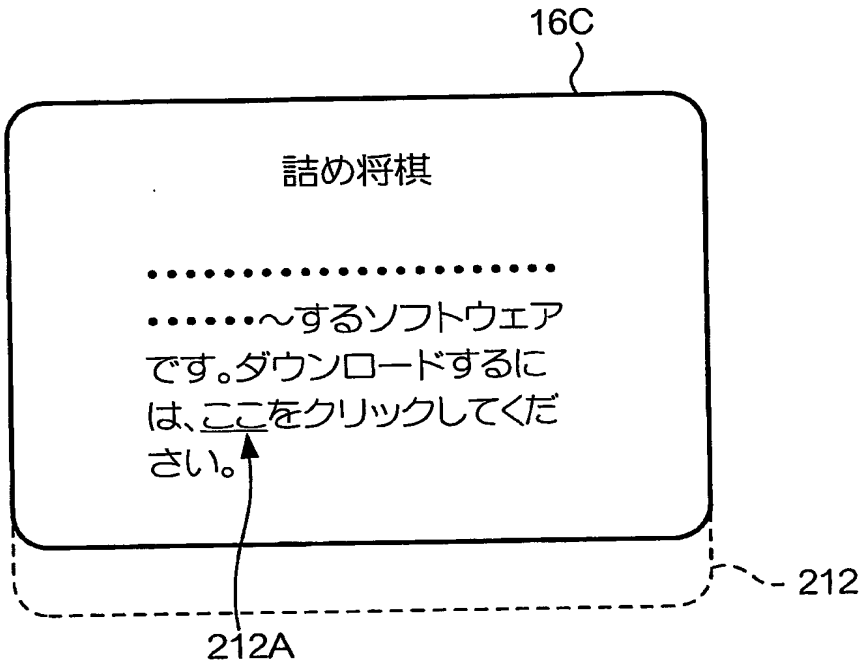


図 13

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
星占い
</OBJECT>
～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。

図 14

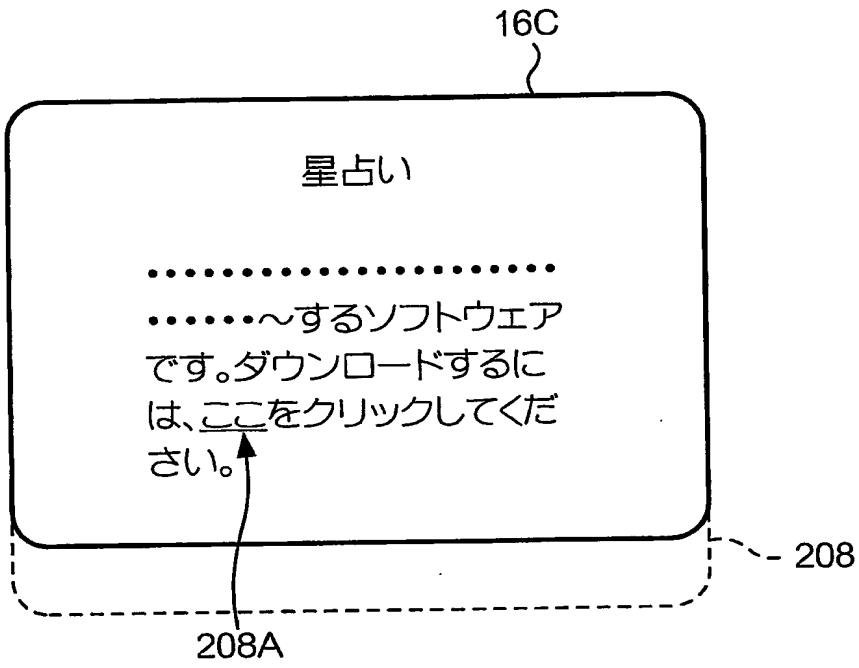


図 15

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/viewer.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
  ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

図 16

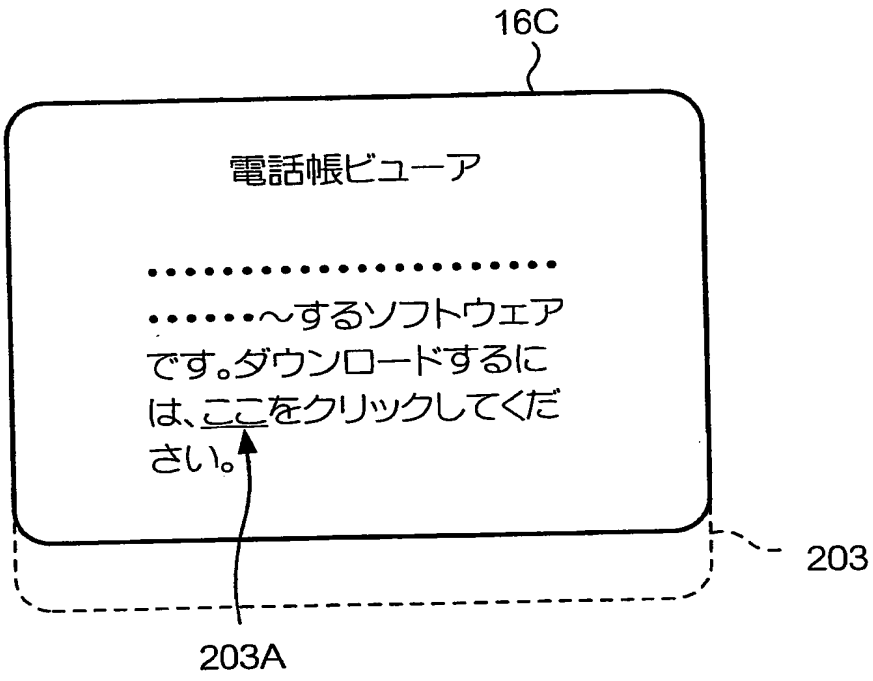

16C
電話帳ビューア
・・・・・・・・・・・・・・・・・・・・・・
・・・・・・～するソフトウェアです。ダウンロードするには、ここをクリックしてください。
203
203A

図 17

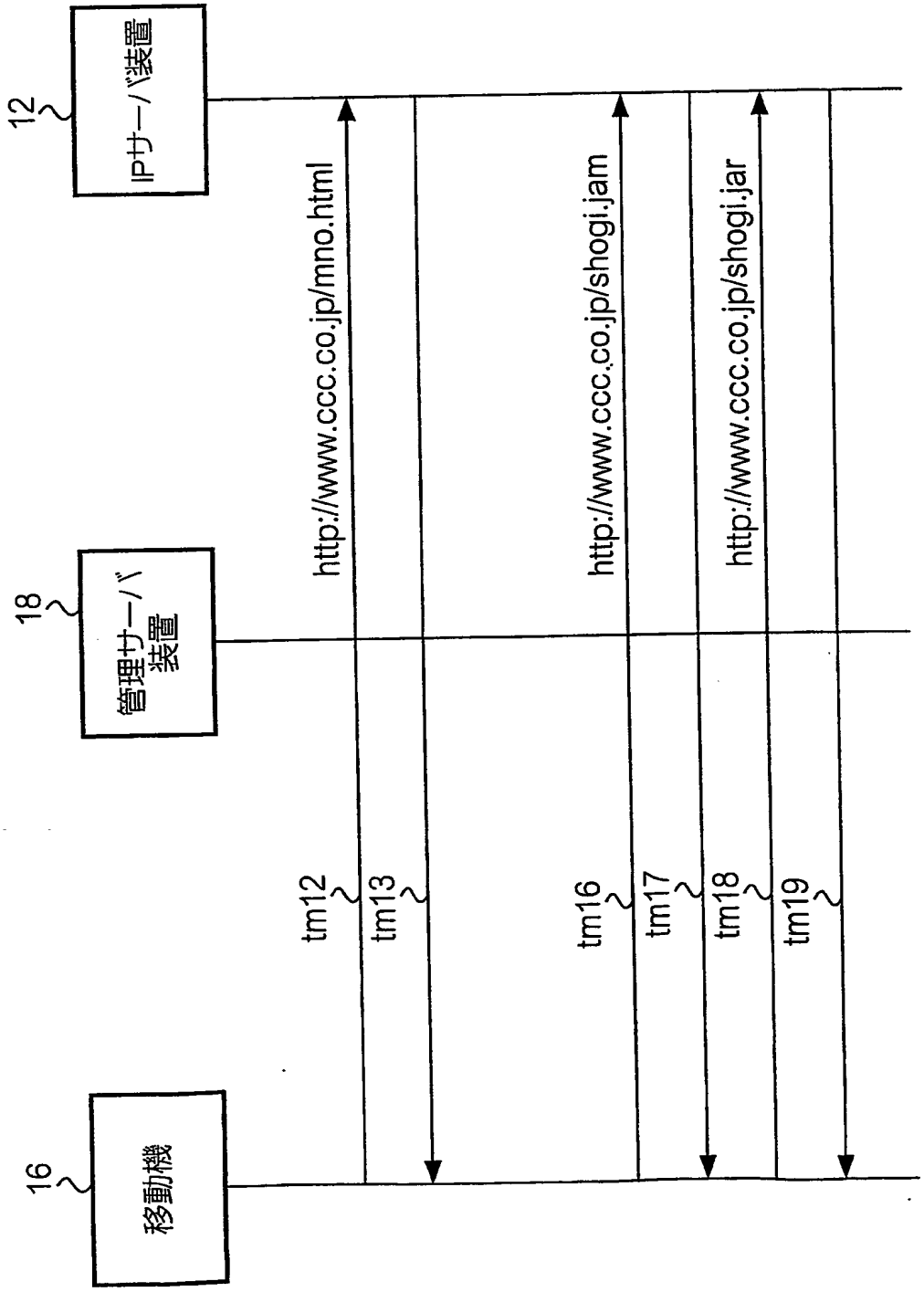

16
移動機
18
管理サーバ装置
12
IPサーバ装置
http://www.ccc.co.jp/mno.html
http://www.ccc.co.jp/shogi.jam
http://www.ccc.co.jp/shogi.jar
tm12
tm13
tm16
tm17
tm18
tm19

図 18

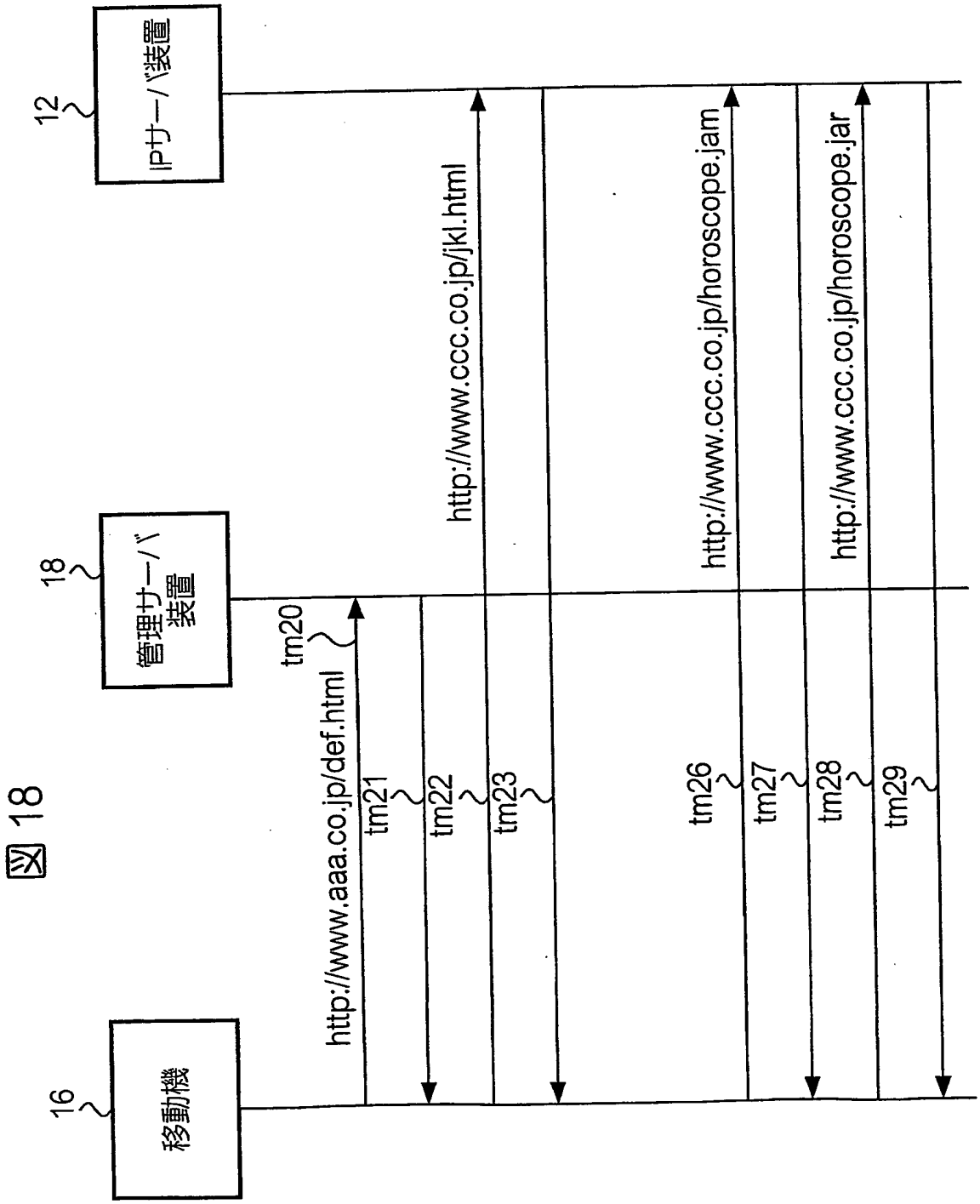

16
移動機
18
管理サーバ装置
12
IPサーバ装置
http://www.aaa.co.jp/def.html
tm20
tm21
tm22
tm23
http://www.ccc.co.jp/jkl.html
tm26
tm27
tm28
tm29
http://www.ccc.co.jp/horoscope.jam
http://www.ccc.co.jp/horoscope.jar

図 19

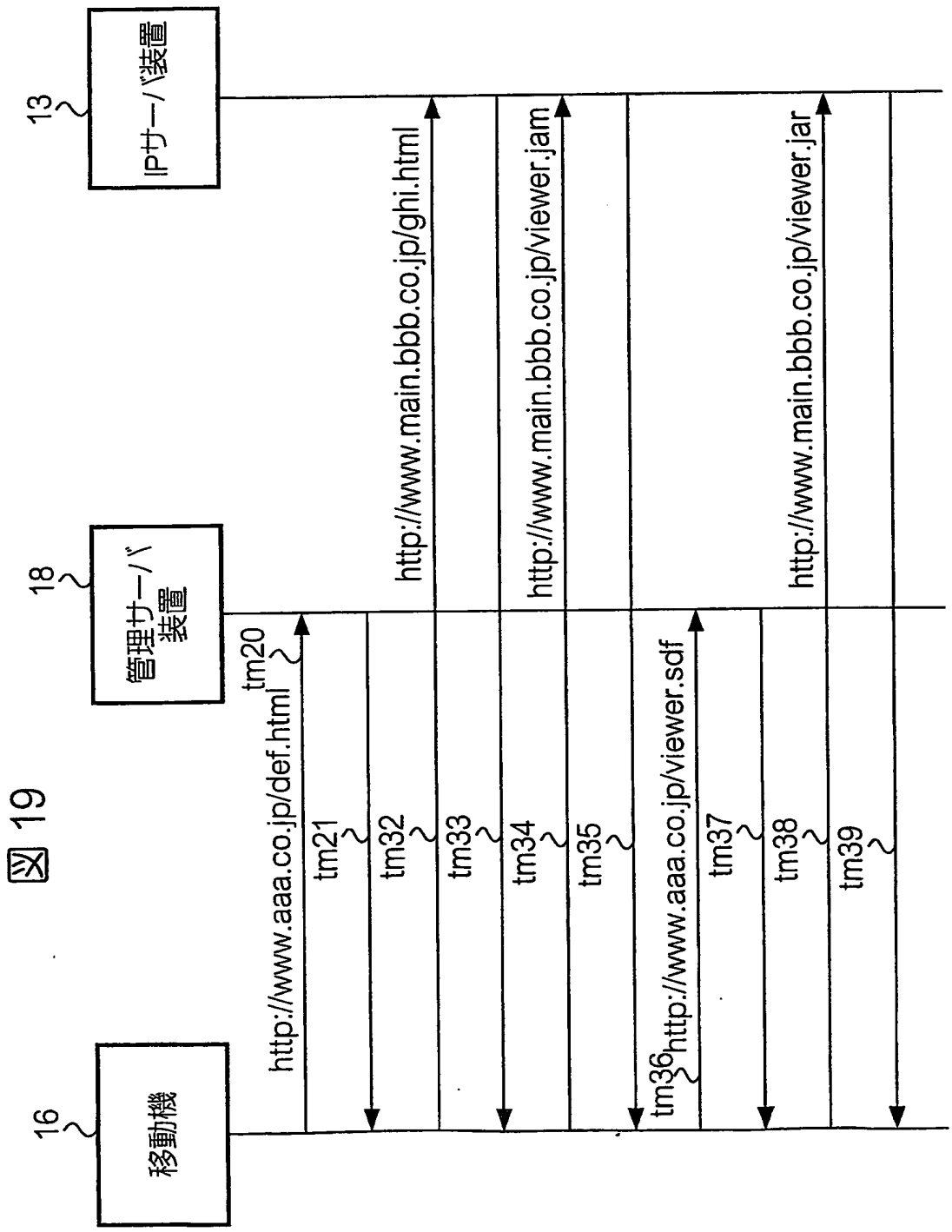

16
移動機
18
管理サーバ装置
13
IPサーバ装置
tm20
http://www.aaa.co.jp/def.html
tm21
tm32
http://www.main.bbb.co.jp/ghi.html
tm33
tm34
http://www.main.bbb.co.jp/viewer.jam
tm35
tm36
http://www.aaa.co.jp/viewer.sdf
tm37
tm38
http://www.main.bbb.co.jp/viewer.jar
tm39

図 20

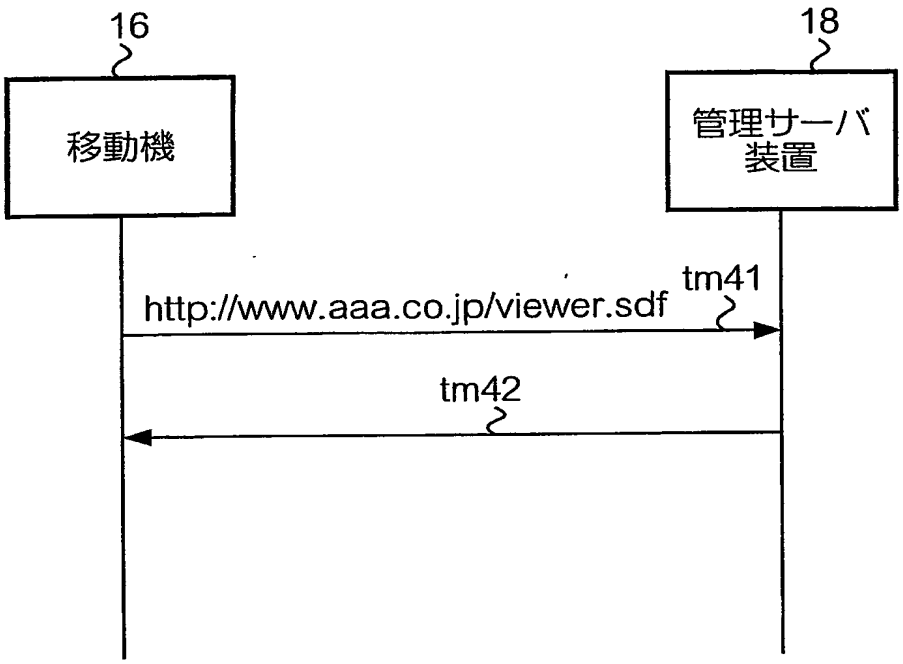

16
18
移動機
管理サーバ
装置
http://www.aaa.co.jp/viewer.sdf
tm41
tm42

図 21

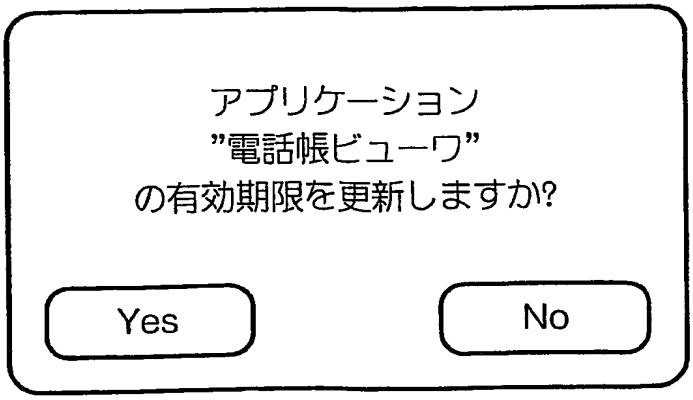

アプリケーション
"電話帳ビューワ"
の有効期限を更新しますか?
Yes
No

図 22

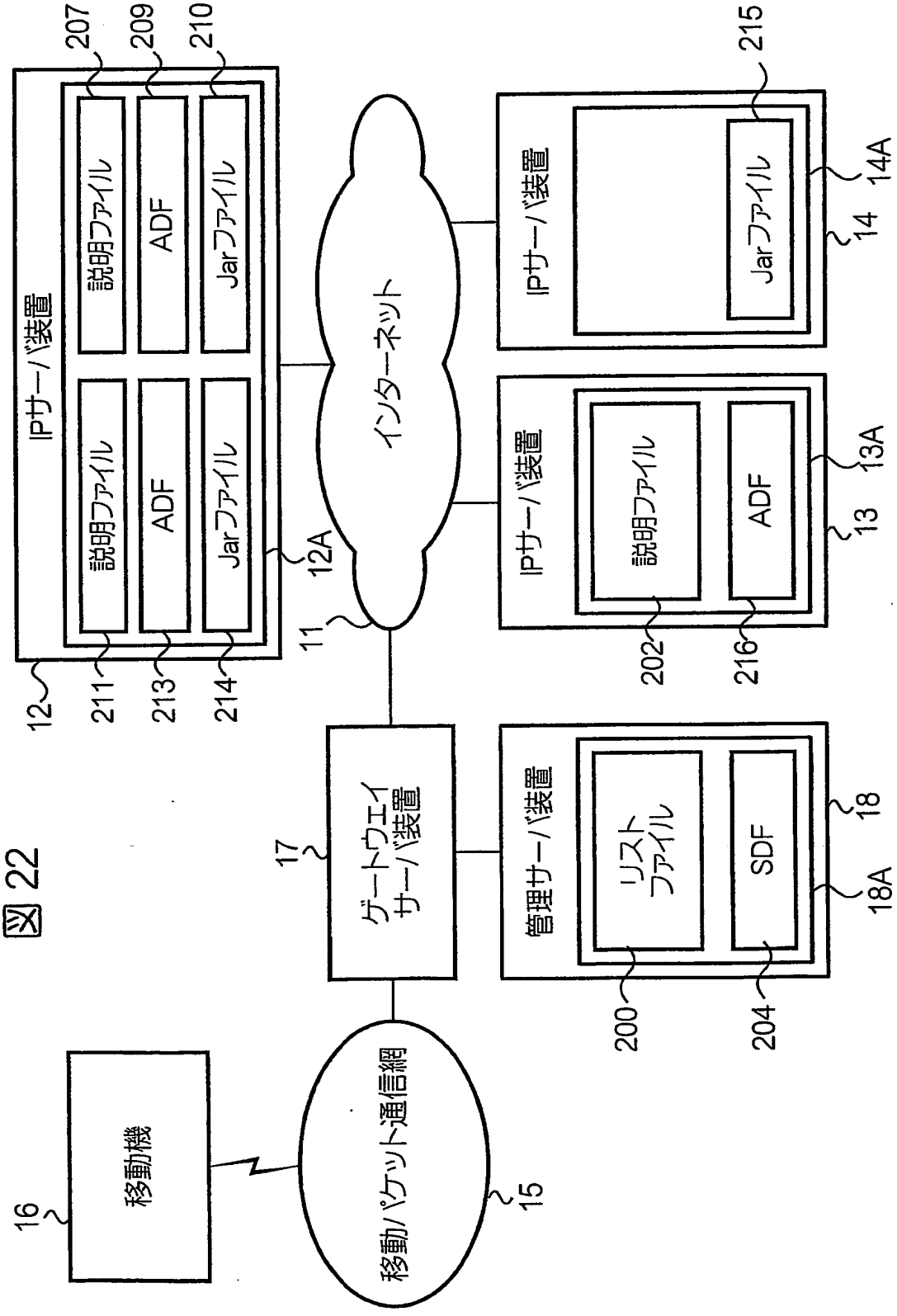
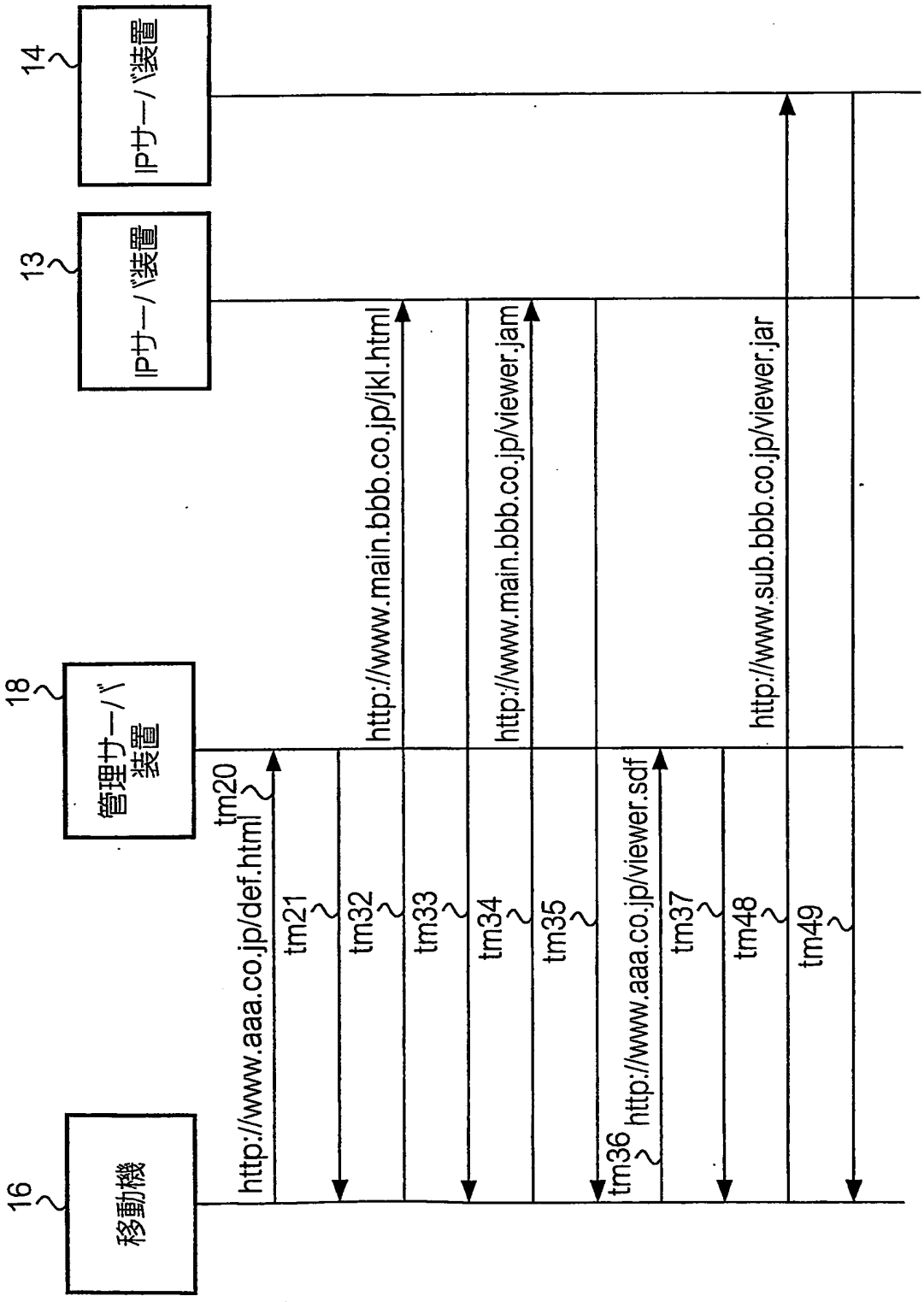

IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
Jarファイル
215
14
14A
IPサーバ装置
説明ファイル
ADF
202
216
13
13A
ゲートウエイ
サーバ装置
17
管理サーバ装置
リスト
ファイル
SDF
200
204
18
18A
移動パケット通信網
15
移動機
16

図 23


16
移動機
18
管理サーバ装置
13
IPサーバ装置
14
IPサーバ装置
tm20
http://www.aaa.co.jp/def.html
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
http://www.main.bbb.co.jp/viewer.jam
tm35
tm36
http://www.aaa.co.jp/viewer.sdf
tm37
tm48
http://www.sub.bbb.co.jp/viewer.jar
tm49

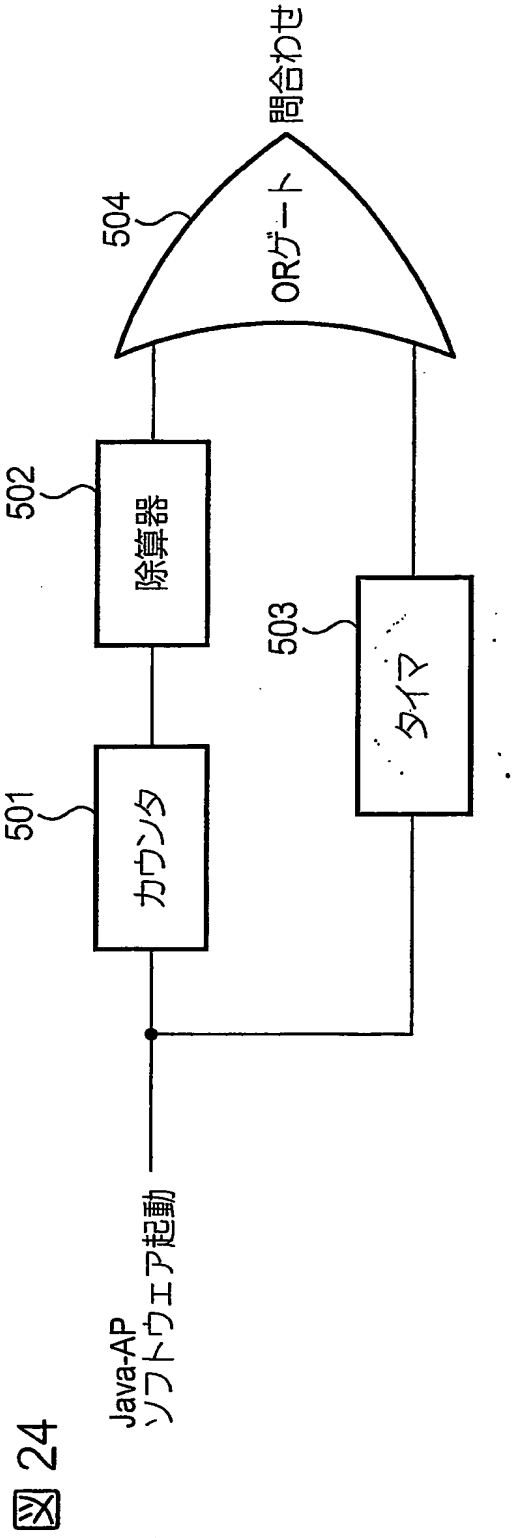

Java-AP
ソフトウェア起動
501
カウンタ
502
除算器
503
タイマ
504
ORゲート
問合わせ

図 24

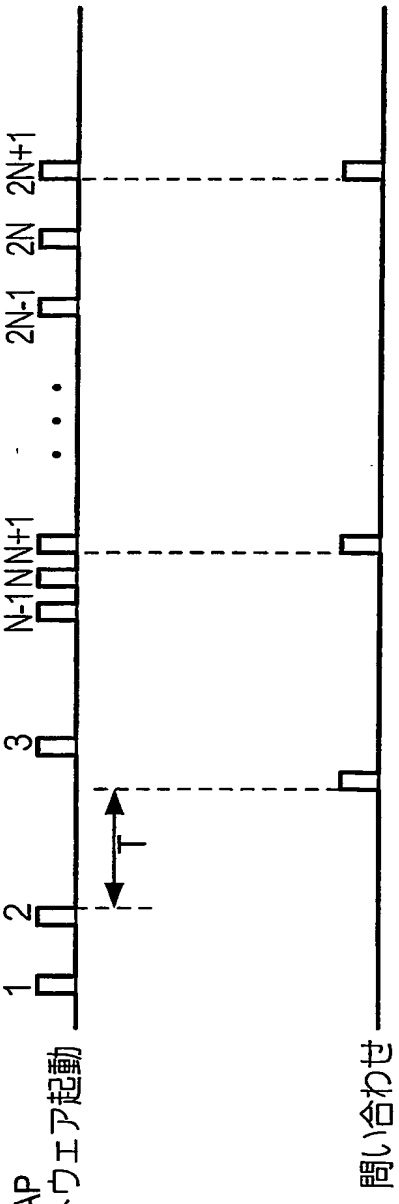

Java-AP
ソフトウェア起動
1
2
3
N-1
N
N+1
2N-1
2N
2N+1
T
問い合わせ

図 25

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/03974

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06, G06F13/00, H04M11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F9/06, G06F13/00, H04M11/00, G06F12/14, G06F15/00, G06F15/16, G06F9/44-9/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS) in Japanese
Computer Software DataBase(Japanese Patent Office) in Japanese
INSPEC(DIALOG) in English

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Edited by ASCII Shoseki Henshubu "i-Mode Java programming - Stand Alone Application Part revised new edition", first edition, Ascii Corp., 21 May, 2001 (21.05.01), ISBN: 4-7561-3790-3, pages 40 to 52(particularly, page 47, table 3-2; page 47, lines 5 to 9; page 48, last line to page 49, line 2)	1-14,16-23 15
Y A	Li Gong, "Java Series Java2 Platform Security", first edition, Kabushiki Kaisha Pearson Education, 30 November, 2000 (30.11.00), ISBN: 4-89471-193-1, pages 123 to 125, 134 to 138 (particularly, page 123, lines 18 to 22; page 124, lines 20 to 22; page 125, section 4.2.2)	1-14,16-23 15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 June, 2003 (10.06.03)	24 June, 2003 (24.06.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/03974

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Computer Today, 01 September, 1998 (01.09.98), Vol.15, No.5, pages 44 to 49, ISBN: 0289-3509 (particularly, page 47, left column, lines 28 to 29, "File Permission", "Socket Permission", "Net Permission")	1-14,16-23 15
A	EP 0813132 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Page 2, lines 20 to 21; page 3, lines 45 to 48 & US 5825877 A & JP 10-083310 A	1-23

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／０３９７４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ９／０６，Ｇ０６Ｆ１３／００，Ｈ０４Ｍ１１／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ９／０６，Ｇ０６Ｆ１３／００，Ｈ０４Ｍ１１／００，Ｇ０６Ｆ１２／１４，
Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１５／１６，Ｇ０６Ｆ９／４４－９／４６

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
ＪＳＴファイル（ＪＯＩＳ）日本語，
ComputerSoftwareDataBase（日本国特許庁）日本語，
ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）英語

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	アスキー書籍編集部・編、「ｉモードＪａｖａプログラミングースタンドアロン・アプリケーション編　改訂新版」、初版、株式会社アスキー、２００１．０５．２１、ＩＳＢＮ：４－７５６１－３７９０－３、ｐｐ．４０～５２（特に第４７頁の表３－２、第４７頁第５～９行、第４８頁末行～第４９頁第２行）	１－１４，１６－２３
Ａ		１５

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１０．０６．０３	24.06.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	久保　光宏	５Ｂ	９１８９
	電話番号　０３－３５８１－１１０１　内線　３５４６		

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０３９７４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	Ｌｉ　Ｇｏｎｇ、「Ｊａｖａ　Ｓｅｒｉｅｓ　Ｊａｖａ２プラットフォームセキュリティ」、初版、株式会社ピアソン・エデュケーション、２０００．１１．３０、ＩＳＢＮ：４－８９４７１－１９３－１、ｐｐ．１２３～１２５及び１３４～１３８（特に第１２３頁第１８～２２行、第１２４頁第２０～２２行、第１２５頁の４．２．２節）	１－１４，１６－２３
Ａ		１５
Ｙ	Ｃｏｍｐｕｔｅｒ　Ｔｏｄａｙ，１９９８．０９．０１，Ｖｏｌ．１５，Ｎｏ．５，ｐｐ．４４～４９，ＩＳＳＮ：０２８９－３５０９（特に第４７頁左コラム第２８～２９行の”ＦｉｌｅＰｅｒｍｉｓｓｉｏｎ”、”ＳｏｃｋｅｔＰｅｒｍｉｓｓｉｏｎ”、”ＮｅｔＰｅｒｍｉｓｓｉｏｎ”という記載）	１－１４，１６－２３
Ａ		１５
Ａ	ＥＰ　０８１３１３２　Ａ２（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｂｕｓｉｎｅｓｓ　Ｍａｃｈｉｎｅｓ　Ｃｏｒｐｏｒａｔｉｏｎ）．１９９７．１２．１７，第２頁第２０～２１行、第３頁第４５～４８行， ＆　ＵＳ　５８２５８７７　Ａ， ＆　ＪＰ　１０－０８３３１０　Ａ	１－２３